



RAS-E

Industrial router & RAS server & firewall

User manual

Document reference : 9016309-04

For the firmware version V2.30 and the following versions

The RAS-E router is manufactured by

ETIC TELECOM
13 Chemin du vieux chêne
38240 MEYLAN
FRANCE

:

TEL : + 33 4-76-04-20-00
FAX : + 33 4-76-04-20-01
E-mail : hotline@etictelecom.com
web : www.etictelecom.com

OVERVIEW

1	PRODUCTS IDENTIFICATION.....	7
2	PRODUCT PRESENTATION.....	8
2.1	Overview	8
2.2	Applications.....	9
2.3	Main features	11
3	TECHNICAL DATA.....	13

INSTALLATION

1	PRODUCT DESCRIPTION	15
1.1	Connectors	19
1.2	DIP-switches & push-button	21
2	VENTILATION.....	21
3	SUPPLY VOLTAGE.....	21
4	ETHERNET PORTS.....	21
5	RS232 INTERFACE	22
6	RS485 INTERFACE	22
7	DIGITAL INPUT & OUTPUT CONNECTION.....	23

SETUP

1	SET UP STEPS.....	25
2	CONFIGURING THE RAS-E ROUTER	26
2.1	Overview	26
2.2	First configuration	27
2.3	Modifying the configuration from the LAN.....	28
2.4	Modifying the configuration from the WAN interface.....	29

... SETUP

3	REBOOTING THE ROUTER AFTER PARAMETERS CHANGES	29
4	RECOVERING THE FACTORY LAN IP ADDRESS	30
5	RECOVERING THE FACTORY CONFIGURATION	30
6	RESTRICTING ACCESS TO THE ADMINISTRATION SERVER	30
7	RECOVERING A FREE ACCESS TO THE ADMINISTRATION SERVER	31
8	FACTORY CONFIGURATION.....	31
9	LAN INTERFACE.....	32
9.1	IP protocol	33
9.2	DHCP server	33
10	WAN INTERFACE.....	35
10.1	IP protocol menu	35
10.2	"Control" menu	36
11	CREATING VPN CONNECTIONS BETWEEN ROUTERS	37
11.1	Principles	37
11.2	IPSec VPN connections	39
11.3	TLS VPN connections.....	45
12	ROUTING FUNCTIONS	51
12.1	Basic routing function	51
12.2	Static routes	52
12.3	RIP protocol.....	53
13	ADDRESS AND PORT TRANSLATION	54
13.1	Port forwarding	54
14	REMOTE USERS CONNECTIONS SERVICE	56

... SETUP

15	REMOTE USERS CONNECTIONS	57
15.1	Principles	57
15.2	Configuring a TLS connection.....	58
15.3	Configuring a PPTP connection	61
16	M2ME_CONNECT SERVICE.....	62
16.1	Overview	62
16.2	Configuring a M2Me_Connect connection	63
17	USERS LIST.....	65
18	FIREWALL	68
18.1	Overview	68
18.2	Main filter	70
18.3	Remote users filters.....	74
19	SERIAL TO IP GATEWAY	79
19.1	Modbus menu	80
19.2	RAW TCP gateway	83
19.3	RAW UDP gateway	85
20	USB TO IP GATEWAY	87
20.1	Principles	87
20.2	Configuration.....	88
21	ADVANCED FUNCTIONS	89
21.1	Adding a certificate.....	89
21.2	Alarms	89
21.3	Configuring the web portal	91
21.4	Configuring the DNS server	92

DIAGNOSTIC & MAINTENANCE

1	DIAGNOSTIC	93
2	SAVING THE PARAMETERS TO A FILE	94
3	UPDATING THE FIRMWARE	95

Appendix 1 : html server overview

Appendix 2 : VPN technology

Appendix 3 : Information which has to be collected to setup the
connection to the M2Me_Connect service

1 Products identification

RAS-E-	1400	1201	1220	1230
IP router	•	•	•	•
Firewall SPI	•	•	•	•
Remote access server - 25 users	•	•	•	•
M2Me_Connect compatibility	•	•	•	•
25 VPN IPSEC & SSL	•	•	•	•
Serial gateway Raw	-	-	-	-
Serial gateway (Raw TCP and UDP, Telnet, Modbus, Unitelway)	-	-	•	•
USB gateway	-	•	-	-
RJ45 10 / 100 BT	4	2	2	2
USB host	-	1	-	-
RS232	-	-	1	2
RS485	-	-	1	-
IP router	•	•	•	•
NAT	•	•	•	•
Port forwarding	•	•	•	•
SNMP	•	•	•	•
DNS	•	•	•	•
DHCP client or server on the LAN interface	•	•	•	•
Digital input for alarm emails	1	1	1	1
HTML setup	•	•	•	•
IO Viewer : optional dynamic data html server	•	•	•	•

The sign • means the function is provided

The sign - means the function is not provided

2 Product presentation

2.1 Overview

The RAS-E is a security product designed to interconnect safely industrial devices with an IP network like a factory or a company network or Internet.

The RAS-E comes with two interfaces :

The LAN interface :

It is made to connect the industrial devices.

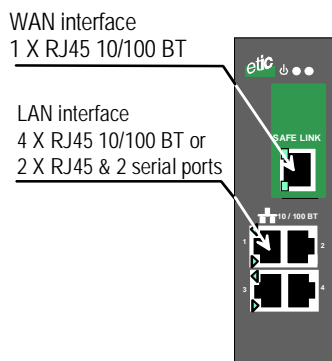
Depending on the model, it includes

- 4 Ethernet ports
- or 2 Ethernet and 2 serial ports
- or 2 Ethernet and 1 USB port.

The WAN interface :

It is a 10/100 BT interface to connect the RAS-E to a company network or a provider network or the Internet.

VPN can be set on that interface between the RAS-E and other routers (25 VPN max.) or between the RAS-E and remote users (25 users max.)

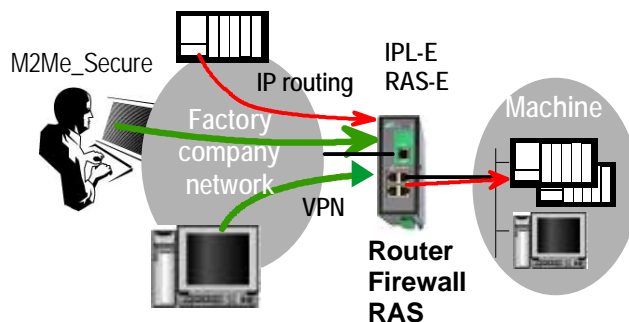


The RAS-E is at the same time an IP router, a VPN client or a VPN server, a remote access server (RAS) and a stateful inspection firewall.

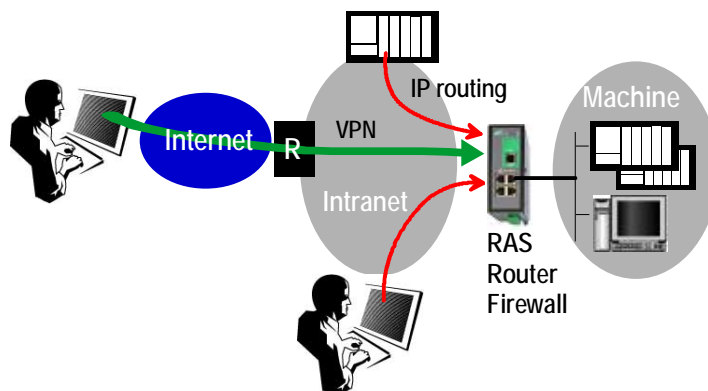
2.2 Applications

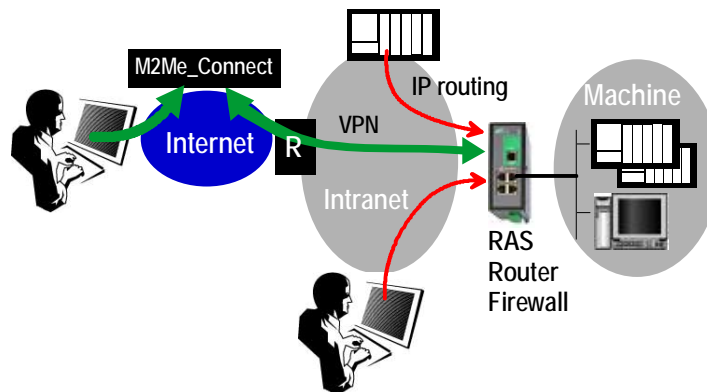
That features in the same product make the RAS-E a top level solution to connect safely a machine to a company network and to provide a secure remote access to the machine.

Safe connection of a machine to a company network :



Remote maintenance ;



Remote maintenance through the M2Me_Connect service :

2.3 Main features

The RAS-E router provides the functions hereafter :
Some features are provided only on particular models.

IP router

The RAS-E firewall-router provides powerful, flexible and comprehensive solutions to route IP packets between the LAN and the WAN interface.

VPNs client or server

The RAS-E router is able to establish safe VPN tunnels.

Once a VPN is established between two RAS-E routers, each IP device connected to the first RAS-E can exchange IP packets with any device connected to the other RAS-E.

The VPN mechanism ensures at the same time end-points authentication, data integrity and confidentiality.

The RAS-E router is able to establish up to 25 IPSec or TLS – SSL VPNs.

Authentication can be carried-out with a pre-shared key or with a certificate.

SPI Firewall

The RAS-E incorporates a stateful inspection firewall.

It is able to check source and destination IP addresses and port numbers for data coming from the WAN interface or from the LAN interface.

Remote access server

Remote users are authenticated, an IP address belonging to the LAN interface is automatically assigned to their PC.

Moreover, The traffic coming from the PC of each remote user is filtered according to the remote user identity.

M2Me_Connect service™ *

The RAS-E is compliant with M2Me_Connect, the remote connection service provided by ETIC TELECOM over the Internet.

Serial gateway *

The product includes an asynchronous (RS232-RS485) to IP gateway, enabling to connect asynchronous or USB devices directly and safely to the Ethernet network.

DHCP client or server

DHCP is a standard Internet protocol that enables a DHCP server to dynamically distribute IP addresses and configuration information to the DHCP clients.

The RAS-E can be a DHCP client or server on its LAN interface or a DHCP client on its WAN interface.

Emails – sms

An email (or SMS) can be sent each time one on the two digital inputs is opened or closed.

SNMP

The RAS-E router is an SNMP agent.

Html and DIP switches configuration

The RAS-E is configured with a web server .

Two DIP switches allow to assign an IP address to the RAS-E over the LAN interface : DHCP client or server, factory IP address or stored IP address.

EticFinder™ software

The ETICFinder software is delivered with the product.

It detects the ETIC products connected to an Ethernet interface and displays the MAC address and the IP address of each product.

M2Me_Secure™ VPN client software

M2Me_Secure is a TLS client able to register up to 100 VPN connections the user can set on a click.

* That feature is provided only on particular models; see the [Product Identification table](#) above

3 Technical data

General characteristics	
Dimensions	137 x 48 x 116 mm (h, l, p)
Electrical safety	EN 60950- UL 1950
EMC	ESD : EN61000-4-2 : Discharge 6 KV RF field : EN61000-4-3 : 10V/m < 2 GHz Fast transient : EN61000-4-4 Surge voltage : EN61000-4-5 : 4KV line / earth
RoHS	2002/95/CE (RoHS)
Supply voltage	10 to 30 VDC – 170 mA at 24 VDC
Operating T°	-20°C / + 60°C Humidity 5 – 95 %
Throughput	Between the WAN interface and the LAN interface : IP router : 10 Mb/s VPN : 2 Mb/s

Ethernet / IP router	
Ethernet	10/100 BT – 2 or 4 switched ports
IP router	Remote connections- static routes – RIP V2
IP address translation	Source IP @ translation (NAT) Destination IP @ translation (DNAT) Port translation (Port forwarding)
DNS	Domain name
IP address assignment	Fixed IP @ or DHCP client or DHCP server

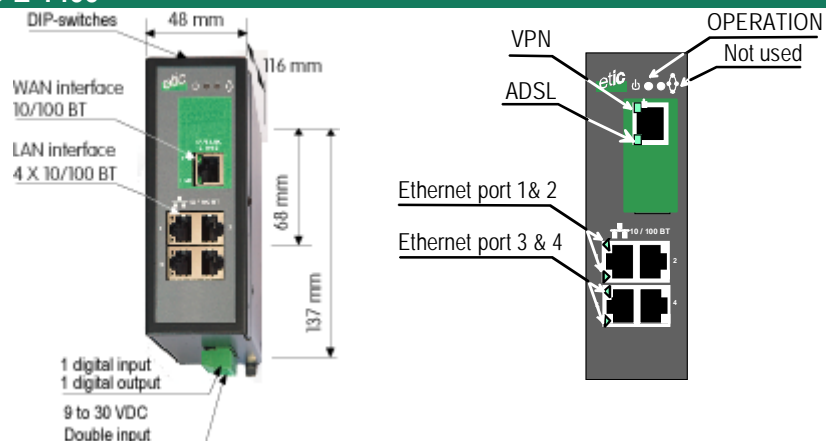
Security	
VPN	Client or server IPSEC or TLS/SSL Encryption 3DES Certificate X509 or preshared key 25 VPNs maximum of the same type (TLS or IPSec)
Firewall	Stateful packet inspection (50 rules)
Logs	Date and time stamped logs


Remote access server (RAS)	
User list	25 users
Connection	VPN PPTP / L2TP-IPSec / TLS Open VPN Login & password Certificate X509
M2Me	VPN Compliant with the M2Me_Secure VPN client Compliant with the M2Me_Connect mediation service
Alarms	3 inputs : emails

Serial interface	
RS232	1200 – 115200 kb/s parity N / E / O RS232 or RS485 (2 wires)
USB	USB host interface
Serial asynchronous to IP gateways	Modbus master and slave Raw TCP client and server Telnet RAW UDP "multicast" unitelway

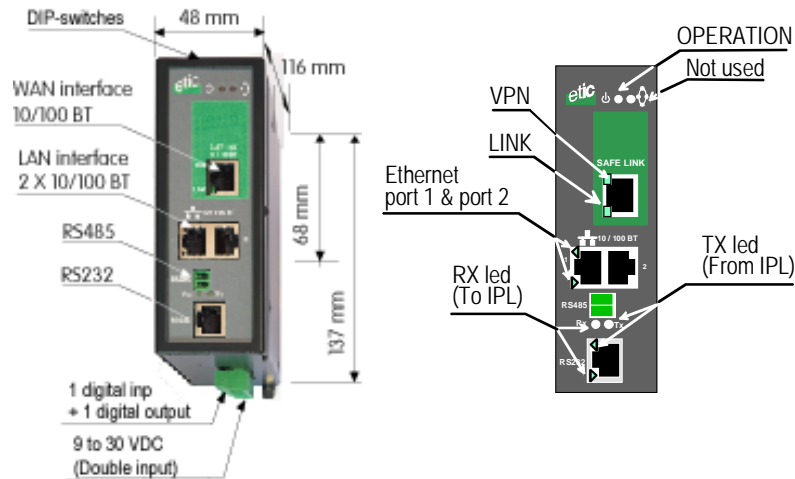
1 Product description


RAS-E-1400

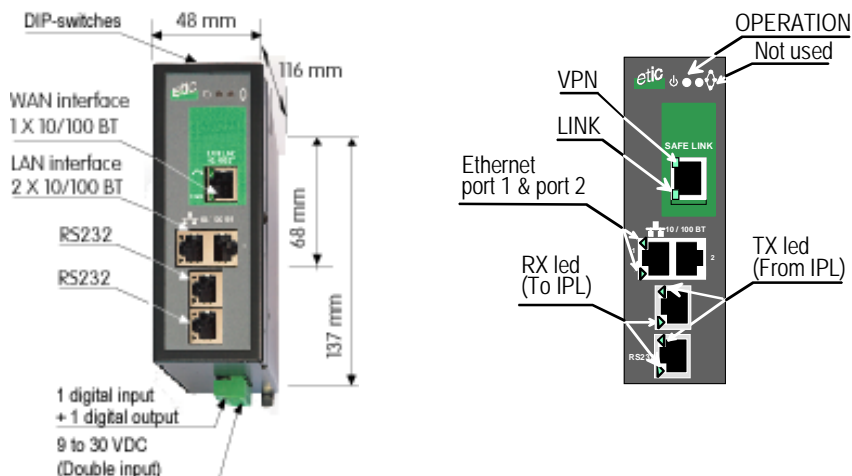



RAS-E-1400		
Interface	Led	Function
WAN	VPN	One VPN at least has been established
WAN	LINK	Blinking quickly : Data activity Lit : Interface connected, no activity
LAN	Ethernet 1 to Ethernet 4	Blinking quickly : Data activity Lit : Interface connected, no activity
		Green : Operation Red : Alarm

RAS-E-1220

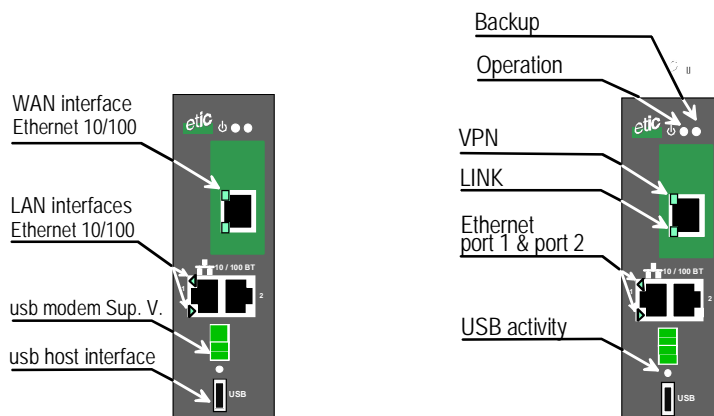



RAS-E-1220		
Interface	Led	Function
WAN	VPN	One VPN at least has been established
WAN	LINK	Blinking quickly : Data activity Lit : Interface connected, no activity
LAN	Ethernet 1 to Ethernet 2	Blinking quickly : Data activity Lit : Interface connected, no activity
RS232	Rx	Bytes received from the RS232 (to the RAS)
	Tx	Bytes transmitted to the RS232 (from the RAS)
RS485	Rx	Bytes received from the RS485 (to the RAS)
	Tx	Bytes transmitted to the RS485 (from the RAS)
		Green : Operation Red : Alarm

RAS-E-1230


RAS-E-1230		
Interface	Led	Function
WAN	VPN	One VPN at least has been established
WAN	LINK	Blinking quickly : Data activity Lit : Interface connected, no activity
LAN	Ethernet 1 to Ethernet 2	Blinking quickly : Data activity Lit : Interface connected, no activity
RS232	Rx	Bytes received from the RS232 (to the RAS)
	Tx	Bytes transmitted to the RS232 (from the RAS)
		Green : Operation Red : Alarm

RAS-E-1201



RAS-E-1201		
Interface	Led	Function
WAN	VPN	One VPN at least has been established
WAN	LINK	Blinking quickly : Data activity Lit : Interface connected, no activity
LAN	Ethernet 1 ↕ Ethernet 2	Blinking quickly : Data activity Lit : Interface connected, no activity
USB		Data activity
		Green : Operation Red : Alarm

1.1 Connectors

8 pins screw block Supply voltage and input / output		
Pin Nr	Signal	Function
1	Power 1 +	Supply voltage input 1 : 10 to 30 Vdc
2	Power 1 -	0 V
3	Power 2 +	Supply voltage input 2 : 10 to 30 Vdc
4	Power 2 -	0 V
5	3V3	+ 3 VDC voltage provided by the product
6	In	Input
7	F +	Output + (max 50Vdc - 0,6A)
8	F -	Output -

WAN RJ45 connector Ethernet 10/100 BT		
Pin Nr	Signal	Function
1	Tx +	TX polarity +
2	Tx -	TX polarity -
3	Rx +	Reception polarity +
4	N.C	-
5	N.C	-
6	Rx -	Reception polarity -
7	N.C.	-
8	N.C.	-

LAN Ethernet RJ45 connector Ethernet 10/100 BT		
Pin Nr	Signal	Function
1	Tx +	TX polarity +
2	Tx -	TX polarity -
3	Rx +	Reception polarity +
4	N.C	-
5	N.C	-
6	Rx -	Reception polarity -
7	N.C.	-
8	N.C.	-

RS485 2 pins screw block (RAS-E-1220)		
Pin Nr	Signal	Function
1	A	RS485 polarity A
2	B	RS485 polarity B

RS232 RJ45 connector (To connect to a DCE to the RS232 port) (RAS-E-1220 or RAS-E-1230)			
Pin Nr	Circuit		Function
1	DTR - 108	OUT	Data terminal ready
2	TD - 103	OUT	Data Emission
3	RD - 104	IN	Data Reception
4	DSR - 107	IN	Data set ready
5	SG - 102	-	Ground
6	Not used	OUT	-
7	CTS - 106	IN	Clear to send
8	RTS - 105	OUT	Request to send

RS232 : RJ45 connector (To connect a DTE to the RS232 port) (RAS-E-1220 or RAS-E-1230)			
Pin	Circuit	Direction	Function
1	CD - 109	OUT	Carrier detect
2	RD - 104	OUT	Data Reception
3	TD - 103	IN	Data Emission
4	DTR - 108	IN	Data terminal ready
5	SG - 102	-	Ground
6	DSR - 107	OUT	Data set ready
7	RTS - 105	IN	Request to send
8	CTS - 106	OUT	Clear to send

1.2 DIP-switches & push-button

DIP switches		
SW 1	SW 2	Management
OFF	OFF	The current IP @ of the product is the stored IP @
ON	OFF	The active IP@ of the product is the factory IP@ : 192.168.0.128 No login and password are required to access to the html server.
OFF	ON	The active IP @ is provided by the BOOTP or DHCP server.
ON	ON	Reserved

Push-button : It enables to restore the factory profile.
To restore the factory profile, switch the power on while pressing the push-button until the RUN light turns green.

Attention : Once the factory profile has been restored, the stored configuration is lost.

2 Ventilation

To avoid overheating when the ambient temperature is high, leave a 1 cm (0.5 inch) space on each side of the product.

3 Supply voltage

The supply voltage must be strictly lower than 30 VDC and higher than 10 VDC. The consumption is 170 mA at 24 VDC.

4 Ethernet ports

The RAS-E features auto-sensing 10/100 Mbps MDI/MDI-X LAN ports.

The upper RJ45 Ethernet connector is the interface on which safe VPN links can be set. It is named the WAN interface.

The other interface (2 or 4 RJ45 depending on versions) are made to connect to a local area network or directly to the industrial devices.

5 RS232 interface

The RS232 data rate can be tuned from 1200 to 115200 b/s with parity (even / odd) or no parity.

The data terminal must be less than 10 meters far from the modem.

Cables can be provided to connect the product to DTE and DCE as follows :

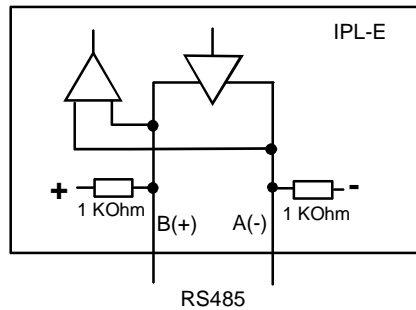
RS232 cables (L=1m)		
Code	User connector	Cable function
CAB592	SubD 9 male	To connect a DCE to the RAS-E
CAB593	SubD 9 female	To connect a DTE to the RAS-E
CAB609	wires	To connect a device providing a specific connector

6 RS485 interface

The RS485 serial interface is provided on the front panel 2 pins screw-block.

Polarisation resistors

1 Kohm bus polarisation resistors are included inside the product.



RS485 line matching

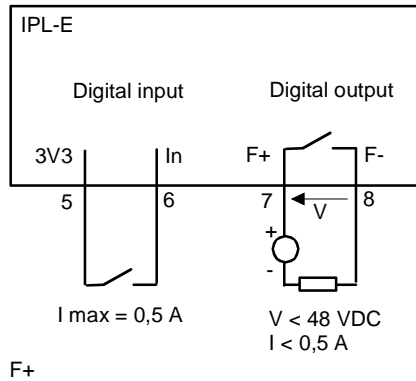
For a several meters long connection over the RS485 local interface, it is not necessary to adapt the RS485 line.

For a longer distance, matching and polarisation resistors must be added.

7 Digital input & output connection

Alarm output

1 relay output is provided to indicate an alarm.
The alarm condition can be selected using the html server.



The electrical characteristics of the output are :

Opto-isolated output

Maximum voltage : 48VDC

Maximum current : 500 mA

Inputs

The product features two digital inputs ; they are not isolated.
if one input is opened, an SNMP trap will be sent to the SNMP server if that function has been enabled.

1 Set up steps

To configure the router, we advise to proceed as follows :

- [Connecting a PC to the router](#)
- [Setting up the LAN interface](#)
- [Setting up the WAN interface](#)
- [Setting up VPNs](#)
- [Setting up routing and IP address translation functions](#)
- [Setting up remote users connections and the M2Me_Connect service](#)
- [Setting up the remote users list](#)
- [Setting up the serial gateway or the USB gateway](#)
- [Setting up the firewall](#)

2 Configuring the RAS-E router

2.1 Overview

Administration server address :

The administration html server is located at the LAN IP address of the router (The default address is 192.168.0.128).

First setup :

For the first configuration, we advise to connect the PC directly to the LAN interface of the RAS-E router.

Setup modifications :

Modifications can be carried out from the LAN interface, or from the Internet if a firewall rule authorises to reach the administration server (not advised), or from the Internet or using a remote user connection or a VPN.

Restoring the factory IP address :

The factory IP address of the router on the LAN interface can be restored by setting the DIP switches SW01 ON and SW02 OFF.

In that position of the DIP switches, the stored configuration is not deleted.

Setting the DIP switches in that position gives also a free access to the administration server from the LAN interface.

During operations, the DIP switches must not be left in that position.

Network IP address :

Later in the text, we often speak of "network address".

We mean the lowest value of the addresses of the network.

For instance, if the netmask of a network is 255.255.255.0, the network address of that network is X.Y.Z.0.

Copy and paste :

Parameters must be entered with the keyboard; they cannot be pasted.

However, it can be useful to paste a string when it is long to avoid errors.

In that case, copy and paste the string, delete the last character of the pasted string, and enter it again with the keyboard.

Saving and restoring the parameters file (see the maintenance chapter)

A parameters file can only be downloaded to a product having the same firmware version.

It is why, we advise to assign a name to a parameter file including the product name and the software version like for instance "myrouterfile_ipLE1220_V241.bin".

2.2 First configuration

Step 1 : Check the DIP switches

Coming from factory, the DIP switches SW1 and SW2 are set OFF to select the stored IP address.

Coming from factory, the stored IP address is the factory IP address 192.168.0.128.

Step 2 : Create or modify the PC IP connection.

Assign to the PC an IP @ in accordance with the RAS-E IP address.

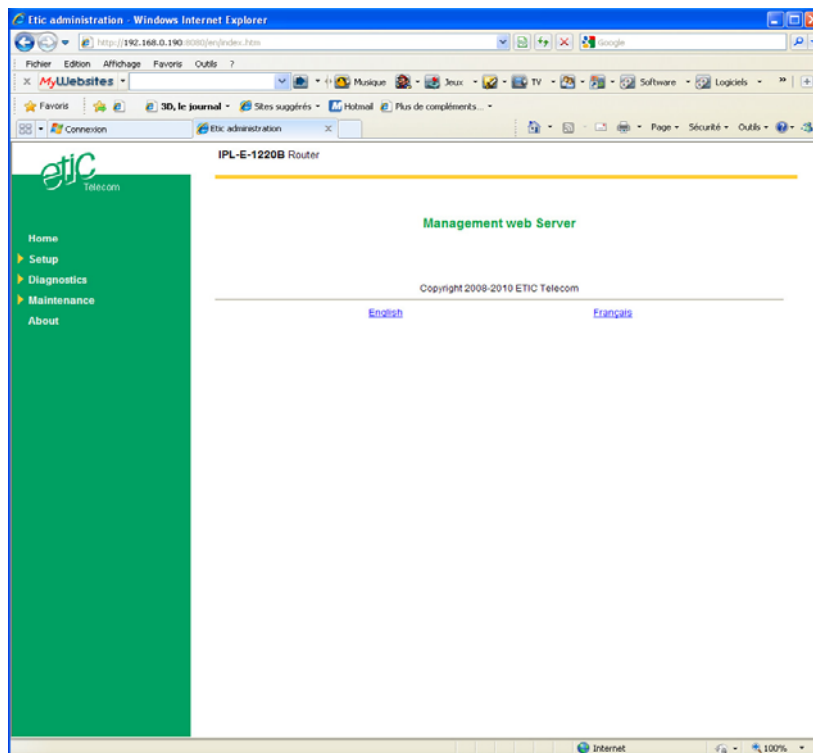
For the first configuration, assign or instance 192.168.0.127 to the PC.

Step 3 : Connect the PC directly to the LAN interface of the RAS-E router using any Ethernet cable (straight or cross wired).

Step 4 : Launch the navigator

Enter the LAN IP @ of the router 192.168.0.128.

The Home page of the administration server is displayed



2.3 Modifying the configuration from the LAN

- If the IP @ of the RAS-E on the LAN interface is assigned by a DHCP server

Step 1 : Ensure the DIP switch SW1 is OFF and SW2 ON to select DHCP client operation.

Step 2 : Launch ETIC FINDER to detect the RAS-E address over the LAN interface.

Click the product once detected.

The Home page of the administration server is displayed.

Remark :

If the home page cannot be displayed, refer [below](#).

- If the IP @ of the RAS-E on the LAN interface is fixed

Step 1 : Ensure the DIP switch SW1 and SW2 are OFF to select the stored IP @.

Step 2 : Launch the html browser and enter the IP address assigned to the router.

Or, launch the ETICFINDER utility to detect the RAS-E address.

Remark :

If the home page cannot be displayed, refer [below](#).

2.4 Modifying the configuration from the WAN interface

Coming from factory, the firewall rejects all the packets coming from the WAN to the LAN.

It is why, it is possible to reach the administration web server from the WAN interface, only if a firewall rule has been created to authorize IP packets exchanges from a WAN IP address to the LAN IP address of the router.

To reach the administration server from the WAN interface, it is also possible to set a remote user PPTP or TLS connection.

Any remote user registered in the User list can reach all the devices of the LAN interface including the router itself unless a User firewall rule has been created to prevent him from reaching the LAN IP address of the router.

3 Rebooting the router after parameters changes

- After the parameters of any page have been completed, click the « Save » button at the bottom of the page.
- After some parameters changes, the RAS-E must restart.
When the configuration has been completely carried out, click the « **Reboot** » red button in the green bar, when displayed.
- Once the product has restarted, check the « **Reboot** » button has disappeared from the green bar.

To save the configuration file to a hard disk :

- Select the “maintenance” menu and then the “Save / restore” menu.
- Click the “Save current configuration to disk” button.

4 Recovering the factory LAN IP address

When launching the html browser, the homepage of the html server may not be displayed; the cause may be the IP address you entered was wrong.

if the IP address you enter is wrong, you can recover the factory IP address by setting SW01 ON and SW2 OFF.

The factory IP address 192.168.0.128 will be restored as long as the SW01 and SW02 micro switch will be left in that position.

Remark :

The SW01 and SW02 must not be left in that position during operations.

5 Recovering the factory configuration

If firewall rules have been created finally preventing from reaching any IP address on the LAN interface including the router itself, it may be necessary to restore the factory configuration of the router.

To restore the RAS-E factory configuration,

- Switch OFF the power supply of RAS-E router.
- Press the push button on the top part of the RAS-E router and switch ON the power supply.
- Keep the push button pressed until the operation led turns red.

Remark : The stored configuration will be lost; the factory IP address 192.168.0.128 will be restored.

6 Restricting access to the administration server

The access to the administration server can be protected by a login and password.

To protect access to the administration server,

- Select the “Setup” menu, the “Security” menu and then the “Administration menu”.

Remark : For more simplicity, we advise to chose the login and the password of one of the remote users stored in the user list.

7 Recovering a free access to the administration server

If the Login & or password entered to reach the administration server have been rejected, it is possible to recover a free access to the administration server from the LAN only, by setting SW01 ON and SW2 OFF.

Remark :

The factory IP address 192.168.0.128 will also automatically be restored as long as SW01 will remain ON and SW2 OFF.

During normal operations SW01 and SW02 must not be left in that position.

8 Factory configuration

Coming from factory, the router configuration is as follows :

LAN IP @	192.168.0.128
WAN IP @	None
Default user :	Login = admin ; Password = admin
Admin. Web server restriction :	None
Firewall :	
Remote user filters	Authorises any remote users belonging to the user list to reach a LAN IP address using a PPTP or TLS connection
Main filter	IP packets coming from the WAN interface to the LAN are dropped
	IP packets transported inside a VPN are forwarded

9 LAN interface

The LAN interface is made of 4 Ethernet switched ports or of 2 Ethernet switched ports and 2 serial ports or 2 serial port and 1 USB port.

On that interface, the following IP addresses must be entered :

The router IP address on the LAN interface *.

The IP address pool assigned to the remote users when they connect.

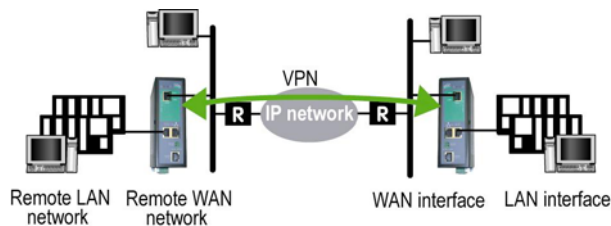
* The administration server is located at that address.

On the LAN interface, the RAS-E can behave like a DHCP server.

Remark about IP addresses assignment rules :

The RAS-E router will be able to route frames between the LAN and the WAN interface only if the IP address assigned to the network connected to the LAN interface is different from the one assigned to the WAN interface.

Moreover , the LAN IP address must be different from the remote LAN IP address



9.1 IP protocol

- Click the « **Configuration** » menu and then « **LAN interface** » and then « **IP protocol** ».

“IP address” parameter :

Enter the IP address assigned to the router over the LAN interface.

That IP address will have to be entered to display the administration server of the router.

“Netmask” parameter :

Enter the IP netmask assigned to the LAN

“Start of users IP address pool” & “end of users IP addresses pool” parameters :

That parameters define the pool of addresses which will be assigned automatically to remote user's PC when they will connect to the router.

Enter the start address and the end address.

Remark :

After the LAN IP address of the router has been modified, it is necessary to reboot the unit.

If VPNs have been created, they must be launched again after the LAN IP address has been modified.

To launch the VPNs again after the LAN IP address has been modified,

- Select the « network » menu and then the « **VPN** » menu,
- Click the « Properties » button in front of the « type of VPN » field, and then on the “OK” button of the window entitled « VPN properties ».
- Click the « Modify » button in front of the « VPN connection » field, and then on the “OK” button.

If the DHCP server is used, it must be launched again after the LAN IP address has been modified.

To launch again the DHCP server after the LAN IP address has been modified,

- Select the « LAN interface » menu and the « DHCP server » menu,
- Unselect the « Enable the DHCP server » checkbox, and then select it again.

9.2 DHCP server

Over the LAN interface, the RAS-E router can behave like a DHCP server.

- **To configure the DHCP server function**, select the « **Setup** » menu and then « **LAN interface** » and then « **DHCP server** ».

“Activate DHCP server” checkbox :

Select that checkbox to enable the DHCP server.

“IP address pool start” & “IP addresses pool end” parameters :

That parameters define the range of IP addresses which can be assigned by the RAS-E to the DHCP client devices.

“Netmask” & “default gateway” parameters :

Enter the netmask of the network connected to the LAN interface and the default gateway address.

“Primary DNS IP address” & “secondary DNS IP address” parameters :

Enter the IP addresses of the domain name servers.; the DHCP server will communicate that information to the DHCP client devices.

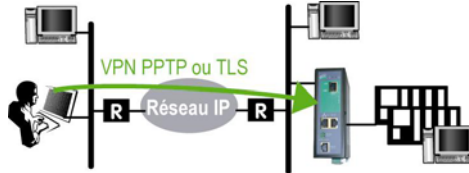
“Client MAC address” “Client IP address” table :

If a fixed IP address must be assigned to the devices connected to the LAN interface, enter the MAC address and the fixed Ip address of each of these devices.

10 WAN interface

The WAN interface is made to connect the RAS-E router to a wide area network (WAN) like a company network or a provider network or the Internet.

VPN can be set on that interface as well between another router (TLS/SSL or IPSec) and the RAS-E, or between remote users and the RAS-E (PPTP or TLS/SSL).



10.1 IP protocol menu

- Select the « **Configuration** » menu and then « **WAN interface** » and then « **IP protocol** ».

“Obtain an IP address automatically” parameter :

Set that option if a DHCP server is in charge of attributing an the IP address of the WAN interface of the router.

Otherwise, enter WAN interface IP address, netmask and default gateway IP address parameters.

“IP address” & “netmask” parameters :

Enter the IP address and netmask assigned to the WAN interface of the router.

“Default gateway” parameter :

Enter the IP address of the default gateway.

“Obtain DNS IP addresses automatically” parameter : Select that option if the Domain name server IP addresses are provided automatically through the WAN interface.

Otherwise, enter the DNS servers IP addresses.

“Primary DNS IP address” & “secondary DNS IP address” parameters :

Enter the IP addresses of the domain name servers.

“Activate network address translation” parameter :

If that option is selected, the source IP address of any frame coming from a device connected to the LAN interface and routed to the WAN interface, is replaced by the router WAN IP address.

“Activate proxy-arp” checkbox :

If that checkbox is selected, the RAS-E will answer to an ARP request

- If it comes from a device connected to the LAN interface,
- and if it concerns a device belonging to the IP network connected the WAN interface.

“SMTP server” parameter :

Enter the SMTP server address (smtp.neuf.fr for instance).

That parameter has to be entered if mails have to be transmitted when an alarm occurs for instance.

“Source account email address” parameter :

Enter the mail address.

10.2 “Control” menu

In that page one can set the parameters which allow to control that the WAN interface is correctly running.

“Enable the ping control” checkbox :

Set that option if a DHCP server is in charge of attributing an the IP address of the WAN interface of the router.

Otherwise, enter WAN interface IP address, netmask and default gateway IP address parameters.

11 Creating VPN connections between routers

11.1 Principles

A VPN tunnel is a safe link set between two end-points routers over an IP network : Both routers authenticate, data are encrypted and each device of a LAN can exchange data with each device of the other one.

To get more explanations about how VPNs work, refer to appendix 1.

25 VPNs can be set on the WAN interface of the RAS-E router.

Two types of VPN can be set : TLS VPN and IPSec VPN.

IPSec has the advantage to be a standard solution.

TLS is easier to employ because the transport layer is TCP or UDP; it is why, it can be easily used when the VPN must pass through several or even numerous company routers.

Once a type of VPN (TLS or IPSec) has been selected, all the VPN set with the RAS-E router will be of the same type.

Two steps are necessary to configure the RAS-E to create VPN connections between routers :

1st step : Select the VPN type and set up the VPN parameters

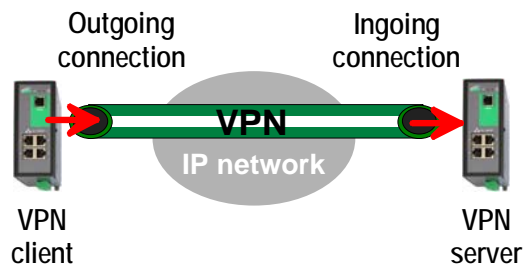
2 types of VPNs can be used to connect RAS-E routers together or with other type of routers: IPSec or TLS/ SSL

Once a type of VPN has been selected, it applies to all the connections with remote routers.

2nd step : Creating VPN connections

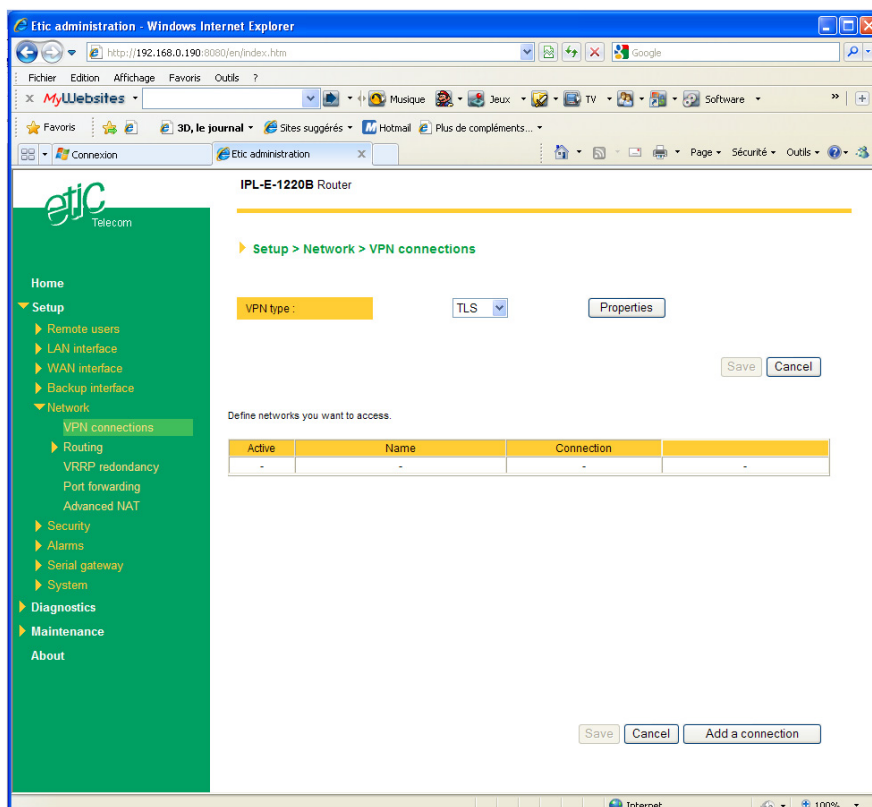
A connection can be an incoming connection or an outgoing connection.

If a connection is an incoming connection, the local router is named "VPN server" and the remote router is a "VPN client".



To create VPN connections between routers,

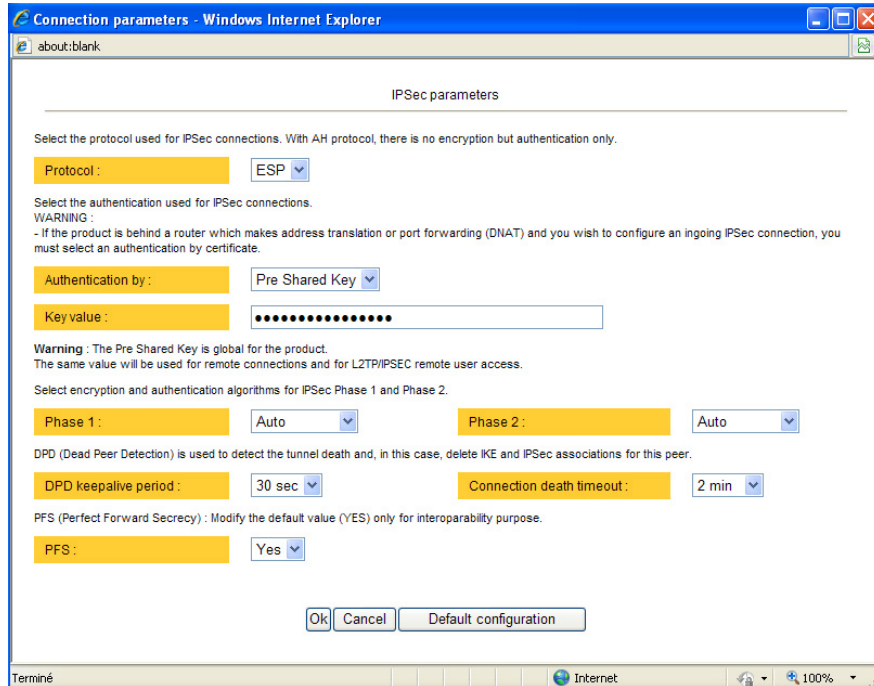
- select the « **Setup** » menu and then « **Network** » and then “**VPN connections**”.



11.2 IPSec VPN connections

11.2.1 Configuring the IPSec protocol

- Select the “**Setup**” menu, the “**network**” menu and then “**VPN connections**”.
- Select the “**Ipsec**” type of VPN,
- Click “**Properties**” .



Connection parameters - Windows Internet Explorer

about:blank

IPSec parameters

Select the protocol used for IPSec connections. With AH protocol, there is no encryption but authentication only.

Protocol : ESP

Select the authentication used for IPSec connections.

WARNING :
- If the product is behind a router which makes address translation or port forwarding (DNAT) and you wish to configure an incoming IPSec connection, you must select an authentication by certificate.

Authentication by : Pre Shared Key

Key value :

Warning : The Pre Shared Key is global for the product.
The same value will be used for remote connections and for L2TP/IPSEC remote user access.

Select encryption and authentication algorithms for IPSec Phase 1 and Phase 2.

Phase 1 : Auto Phase 2 : Auto

DPD (Dead Peer Detection) is used to detect the tunnel death and, in this case, delete IKE and IPSec associations for this peer.

DPD keepalive period : 30 sec Connection death timeout : 2 min

PFS (Perfect Forward Secrecy) : Modify the default value (YES) only for interoperability purpose.

PFS : Yes

Ok Cancel Default configuration

Terminé

Internet 100%

“ Protocol ” parameter :

AH ((RFC2402) provides integrity, authentication, replay resistance and non-repudiation but not encryption.
select AH, if no encryption is required or if NAT traversal is required.

ESP provides the same services plus encryption.

If ESP is selected, an encryption and an authentication protocols must be selected.

“Authentication & encryption key” parameters :

Authentication and encryption can be carried-out with a pre-shared key or a certificate.

“Pre-shared key” value :

The pre-shared key value applies to all the connections.

The maximum length of the key is 40 characters.

The same pre-shared key value will be used for remote users L2TP / IPSec connections.

“Certificate” value

The RAS-E router is delivered with a certificate stored into the product in our factory.

To add a certificate, refer to the “Security” menu.

“Encryption and hash algorithm phase 1” & “Encryption and hash algorithm phase 2” parameters :

These parameters allow to define the encryption and hash algorithms in use during the phase 1 of the exchanges between the end-points (VPN set-up) and during the phase 2 (data exchange).

The default value is Auto; in that case both end-points will negotiate a common algorithm.

“DPD request period” parameters :

A DPD request (also called Keepalive message) is a message sent periodically by each end-point to the other one to make sure that the VPN must be left active.

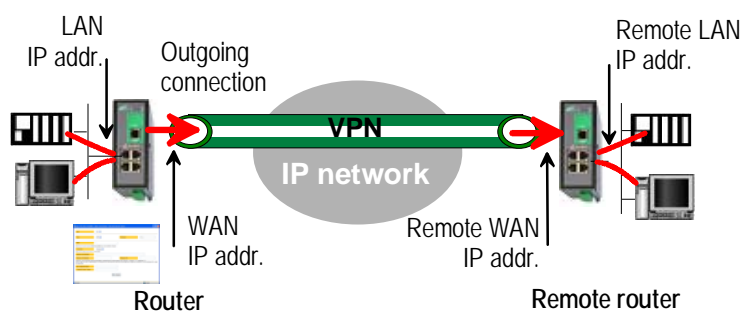
This parameter sets the amount of time (in seconds) between two of these requests.

“Connection death time-out” parameters :

This parameter defines the maximum amount of time (in seconds) a VPN connection will stay established if no traffic or no DPD request message are received from the remote point.

ATTENTION : Once the parameters of the IPSEC connection have been selected, click the OK button and then the Save button.

11.2.2 Configuring an outgoing IPsec connection



To set an outgoing VPN connection,

- Come back to the “VPN connections” screen,
- Click the “add a connection” button.

Remote connection configuration - Windows Internet Explorer

about:blank

Active : ☒ Yes

Protocol : IPSec

Name :

Select the connection (Ingoing or Outgoing) you wish to configure.

Connection : Outgoing

Informations about the remote network.

Remote WAN IP address :

Remote LAN address : Remote LAN netmask :

You choose an authentication using Pre Shared Key
You can use a different key for each connection by filling the parameters below. Otherwise, this is the global key, defined in the IPsec server parameters, which will be used.

Use a specific key for this connection : ☐

Key value :

My WAN IP address :

Ok Cancel

Give a name to the connection and select the “Outgoing” option.

‘Remote WAN IP address’ parameter :

Enter the IP network address and netmask assigned to the remote router over its WAN interface..

“Remote LAN address & Remote LAN netmask” parameters :

Enter the IP network address and netmask assigned to the remote LAN.

- **Preshared key**

If the preshared key used by the connection is the general PSK entered in the “VPN” menu, no additional parameter has to be entered.

If a particular PSK must be used, complete the configuration of the connection as explained below.

“Unique PSK for this node” parameter :

Select that option if a particular PSK key has to be used for this connection.

“PSK value” parameter :

Enter the value of the PSK.

“My WAN address” parameter :

Enter the IP address of the router on the WAN interface.

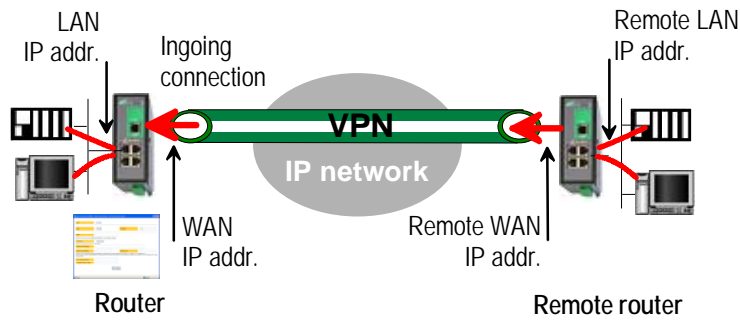
- **Certificate**

“My subjectAlt name” & “Remote subjectAlt name” parameters :

Paste the field "SubjectAltName" of the active certificate of the router you are configuring and the one the remote router.

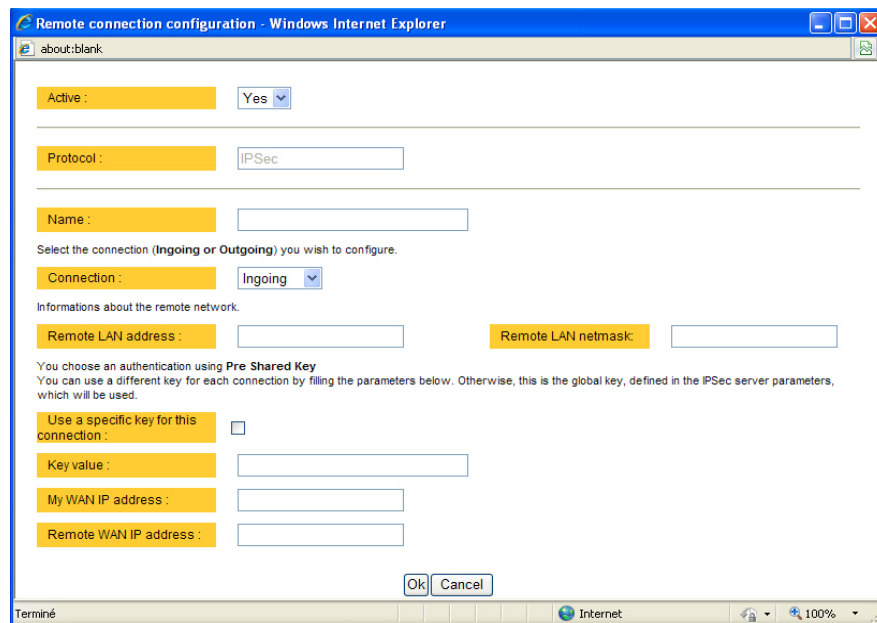
Attention : For ETIC certificates, this field is the Email field

11.2.3 Configuring an incoming IPSec connection



To set an incoming VPN connection,

- Come back to the “**VPN connections**” screen,
- Click the “add a connection” button.



Give a name to the connection and select the **“incoming” connection direction option**.

“Remote WAN IP address” parameter :

Enter the IP network address and netmask assigned to the remote router over its WAN interface.

“Remote LAN address” & “Remote LAN netmask” parameters :

Enter the IP network address and netmask assigned to the remote LAN.

- **Preshared key**

If the key used by the connection is the general PSK entered in the VPN menu, no additional parameter has to be entered.

If a particular PSK must be used, carry out the configuration of the connection as explained below.

“Use a specific key for this connection” parameter :

If that option is not selected, the preshared key entered in the VPN configuration screen will be used by the router.

If that option is selected, enter the specific key.

“My WAN address & Remote WAN address” parameters :

Enter the WAN IP address of the router and the WAN IP address of the remote router.

Attention : For ETIC certificates, this field is the Email field

- **Certificate**

“My subjectAlt name” & “Remote subjectAlt name” parameters :

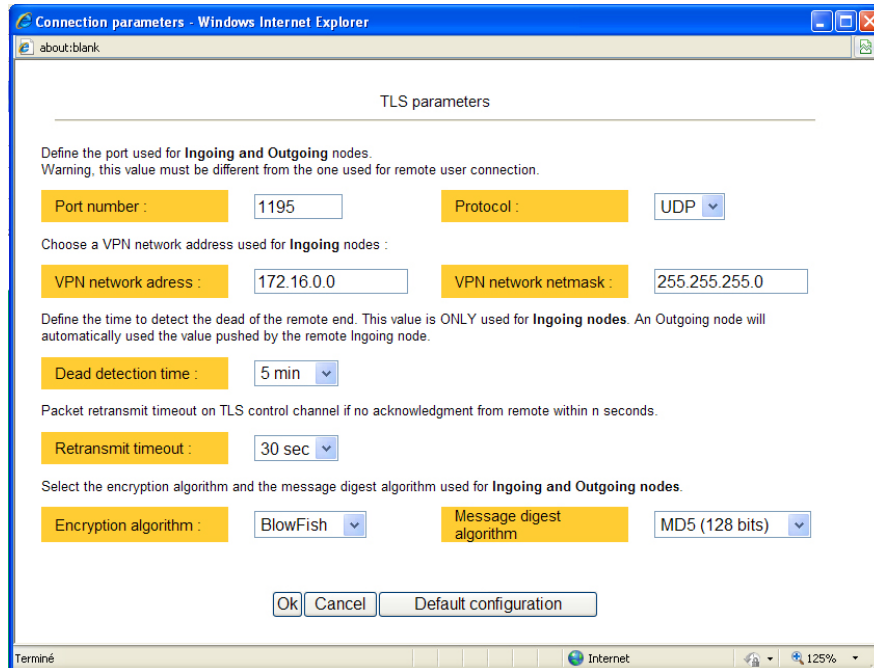
Paste the field "SubjectAltName" of the active certificate of the router you are configuring and the one the remote router.

Attention : For ETIC certificates, this field is the Email field.

11.3 TLS VPN connections

11.3.1 Configuring the TLS-SSL protocol

- Select the “**Setup**” menu, the “**network**” menu and then the ‘VPN connections’ menu.
- Select the “**TLS**” VPN type and click “Properties” .



Connection parameters - Windows Internet Explorer

about:blank

TLS parameters

Define the port used for **Ingoing and Outgoing nodes**.
Warning, this value must be different from the one used for remote user connection.

Port number : 1195 Protocol : UDP

Choose a VPN network address used for **Ingoing nodes** :

VPN network address : 172.16.0.0 VPN network netmask : 255.255.255.0

Define the time to detect the dead of the remote end. This value is **ONLY** used for **Ingoing nodes**. An Outgoing node will automatically used the value pushed by the remote Ingoing node.

Dead detection time : 5 min

Packet retransmit timeout on TLS control channel if no acknowledgment from remote within n seconds.

Retransmit timeout : 30 sec

Select the encryption algorithm and the message digest algorithm used for **Ingoing and Outgoing nodes**.

Encryption algorithm : BlowFish Message digest algorithm : MD5 (128 bits)

Ok Cancel Default configuration

Terminé Internet 125%

“Port number” & “protocol” parameters :

Select the port Nr and the type of level 3 protocol used to transport the TLS VPN; UDP will be preferred.

Attention :

The port number value must be different from the one used by remote users.

“VPN network address” & “VPN network netmask” parameters :

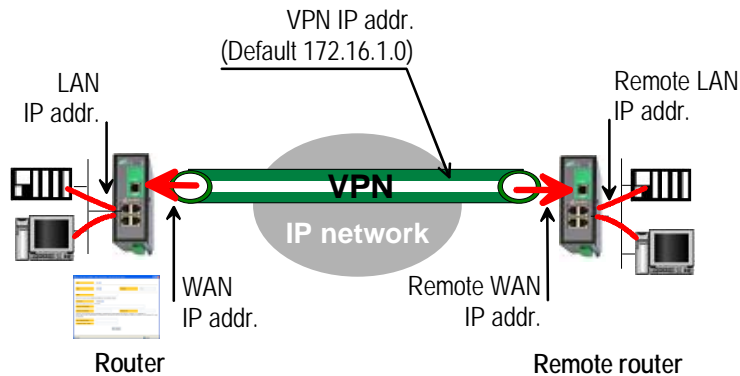
The TLS VPN server router assigns automatically an IP address to the VPN client router.

That VPN IP address must not be confused with the WAN interface IP address.

Attention :

The VPN IP network address field must be different from the WAN network IP address .

The number of VPN addresses cannot be greater than 255; the netmask cannot exceed 255.255.255.0.



“Connection death time-out” parameter :

This parameter defines the maximum amount of time (in seconds) a VPN connection will stay established before being cleared if no response to the VPN control message has been received from the remote router.

“Packet retransmit time-out” parameter:

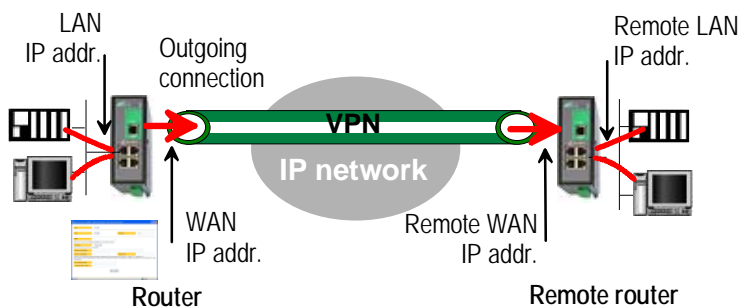
A control message (also called Keepalive message) is sent periodically by the VPN server router to make sure that the VPN must be left active.

This parameters sets the amount of time (in seconds) the server will wait for the response before repeating it.

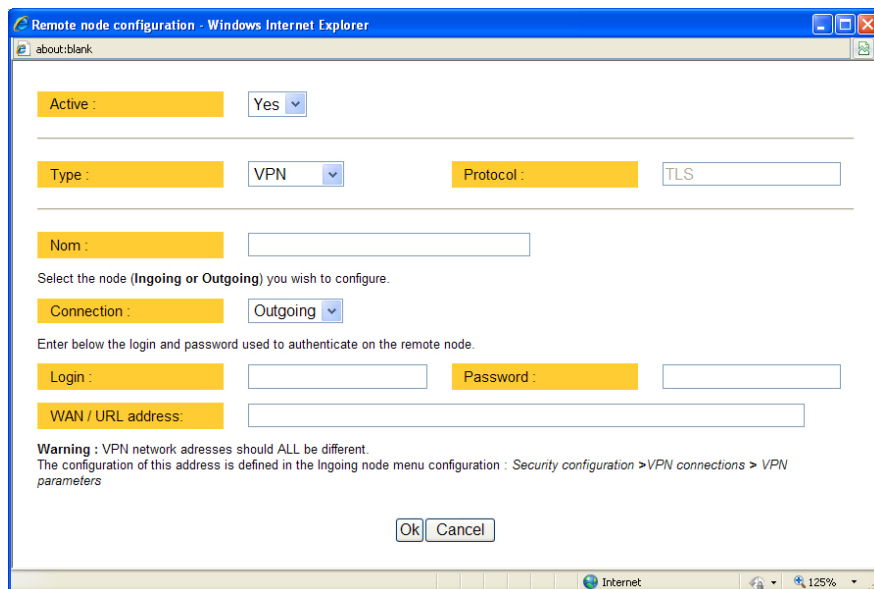
“Encryption algorithm” & “Authentication algorithm” parameter :

That parameters allow to define the encryption and hash algorithms in use.

11.3.2 Configuring an outgoing TLS connection



- Select the **“Setup”** menu, the **“network”** menu and then the **“VPN connections”** menu.
- Click the “add a connection” button.
- Give a name to the connection and select the **“Outgoing”** connection direction option.



“Login & Password” parameter:

Enter the login and password, the router will have to use to authenticate.

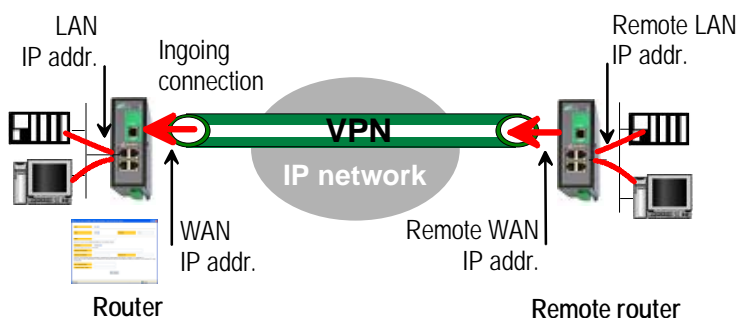
Remote WAN IP address / URL parameter :

Enter the IP address of the remote router or its DNS name.

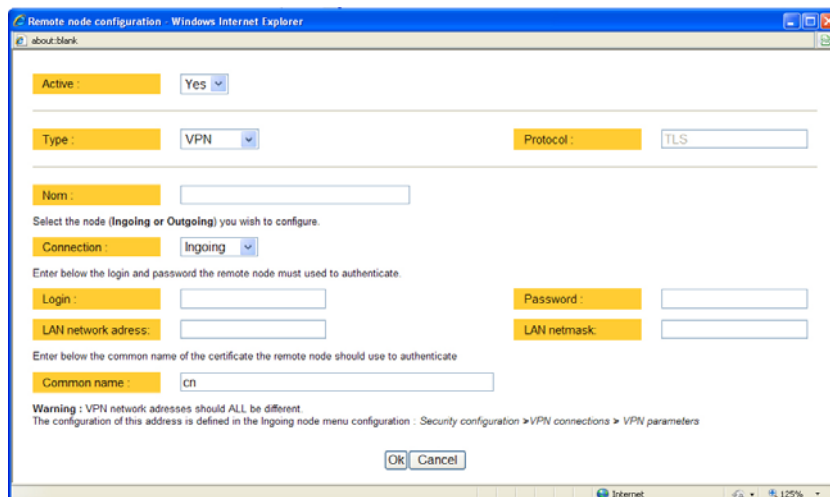
“Remote WAN IP address” ” parameters :

Enter the IP network address and netmask assigned to the remote router over its WAN interface.

11.3.3 Configuring an incoming TLS connection



- Select the **“Setup”** menu, the **“network”** menu and then the **“VPN connections”** menu.
- Click the **“add a connection”** button.



Give a name to the connection and select the **“incoming” connection direction** option.

“Remote router Login” & “Remote router password” parameters :

Enter the login and password of the remote router

The remote router has to use that login and password to authenticate.

“Remote LAN address” & “Remote LAN netmask” parameters :

Enter the IP network address and netmask assigned to the remote LAN.

“Common name” parameters :

Enter the remote router certificate common name.

Attention : For ETIC certificates, this field is the Email field.

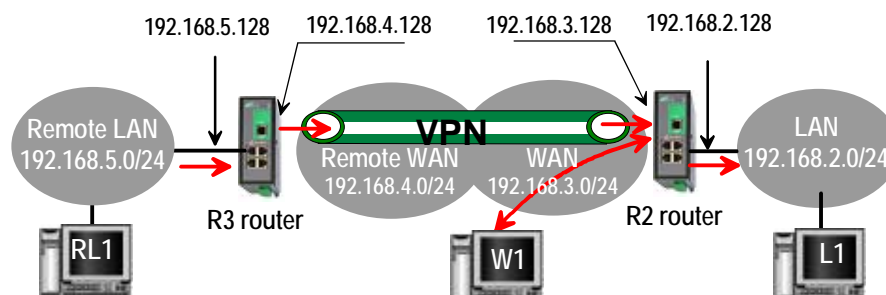
12 Routing functions

12.1 Basic routing function

Once an IP address has been assigned to the R2 router on the LAN interface and another one on the WAN interface (see drawing hereafter), the RAS-E R2 router is ready to route frames ...

... between devices connected to the remote LAN network like RL1, and devices connected to the LAN network like L1 through a VPN;

... between devices connected to the WAN network like W1, and devices connected to the LAN network like L1

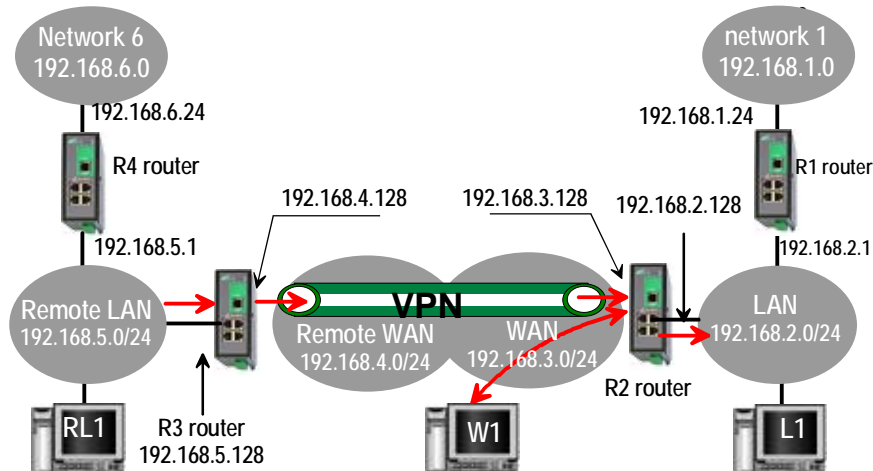


Remark 1 : Firewall rules must be set to authorize WAN to LAN transfer.

Remark 2 : A default gateway address must be entered in each device of the different networks.

12.2 Static routes

However, the router R2 is not able to route frames between a device like L1 belonging to the LAN network and a device connected to “network 6” (see the drawing hereafter).



In that case, it is necessary to enter the route to that hidden “network 6”; that route is called a static route.

A static route consists in a table which describes a destination network (IP address and netmask) and the IP address of the neighbour router through which an IP packet to that destination must pass.

Router 2 static routes :

Active	Route name	Destination	Netmask	Gateway
Yes	Network 6	192.168.6.0	255.255.255.0	192.168.5.1
Yes	Network 1	192.168.1.0	255.255.255.0	192.168.2.1
Yes	Network Remote WAN	192.168.4.0	255.255.255.0	192.168.5.128

Remark :

It is not necessary to enter in the router R2 the static route to the WAN network nor to the remote LAN network, that routes have been automatically created by the router respectively when the WAN IP address has been entered and when the VPN has been configured.

To set a static route,

- Select the “**Configuration**” menu, the “**network**” menu the “**Routing**” menu and then “**Static routes**”.
- click the “Add a route” button.

“Destination IP address” & “netmask” parameters :

Enter the destination network IP address and netmask.

“Gateway IP address” parameters :

Enter the Ip address of the gateway through which the IP packets intended for that network must pass.

12.3 RIP protocol

RIP (**Routing Information Protocol**) is a routing protocol which enables each router belonging to a network to acquire the routes to any subnet.

The principle is as follows :

Routing table

Each router holds a routing table.

Each entry of the table consists in the destination subnet address and the adjacent router address leading to that subnet.

Routing table broadcasting :

Each router broadcasts its table.

Routing table update :

Each router updates its own table using the tables received from the other ones.

To enable RIP,

- select the « **Setup** » menu, the “Routing” menu and then the “RIP” menu».
- Select the ‘Enable RIP on LAN interface’ and the “Enable RIP on WAN interface” options.

13 Address and port translation

The RAS-E provides the capability to replace the original source IP address and the destination port and IP address in particular situations.

13.1 Port forwarding

The port forwarding function consists in transferring to a particular device connected to the LAN interface a particular data flow addressed to the RAS-E router on its WAN interface.

That function applies only to the frames addressed to the WAN IP address of the router.

The transfer criteria is the port number; the port number is used as an additional address field.

When a frame is addressed to the RAS-E router with a particular registered port, it is transferred to a particular device connected to the LAN interface.

Example :

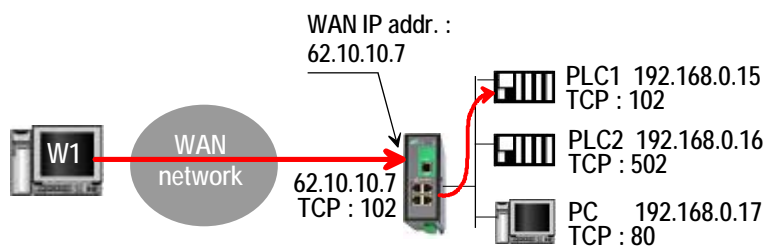
Let us suppose the PC named “W1” of the WAN network has to send frames to the device PLC1 of the LAN network

Suppose moreover that the addresses of the LAN network cannot be used on the WAN network for any reason.

The solution can be to use the Port forwarding function :

When W1 needs to transmit frames to PLC1, it addresses the frames to the RAS-E router on a chosen and agreed port.

The router checks the frame, replaces the destination address by the IP address of the device on the LAN interface, and eventually changes the port number.



The port forwarding rule will be

Internet / WAN	LAN translation	
Service	Device	Service
102	192.168.0.15	102
502	192.168.0.16	502
80	192.168.0.17	80

To set the Port forwarding function,

- select the “network” menu and then the “Port forwarding” menu.
- Click “Add a DNAT” rule.

14 Remote users connections service

The RAS-E provides a full remote user connection function called RAS :

- The remote user authenticates using the login, password and eventually a certificate; the router accepts the connection only if the remote user belongs to the user list.
- Individual access rights are automatically allocated to the remote user.
- An IP address belonging to the LAN network is automatically assigned to the remote PC.
- Data are encrypted (TLS and L2TP / IPSec only).
- The connection is logged.
- Moreover, the RAS-E is compatible with the M2Me_Connect service when setting a direct connection is not possible.

To setup the remote user connection service, the following steps must be carried out :

- Step 1 :

Configure a [PPTP or TLS or L2TP connection](#)

or select the [M2Me_Connect service](#) menu.

- Step 2 :

Complete the [user list](#)

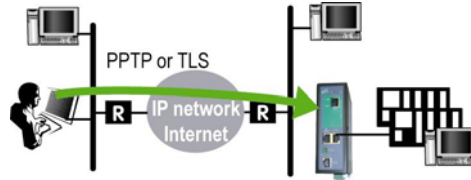
- Step 3 ::

Define the [firewall rules](#) to limit the rights of the remote users

15 Remote users connections

15.1 Principles

A remote user connection is a tunnel set between a remote PC and a router providing the RAS function (Remote Access Service), like the RAS-E.



A remote user connection provides security and simplicity advantages :

- The remote user is identified with a login in and password or eventually a certificate.
- The data is encrypted (TLS or L2TP).
- An IP address belonging to the local network is automatically assigned to the remote user's PC.

The RAS-E manages PPTP and TLS or L2TP remote connections.

Only one type can be selected. It will apply to all the remote users connections.

A PPTP is the simplest type of remote user connection; data is not encrypted.

The remote user can be identified only with a login and password.

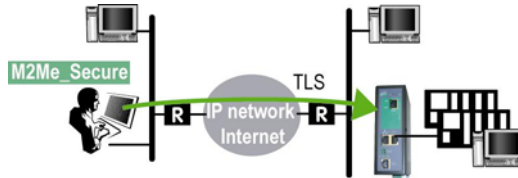
A TLS connection provides encryption; moreover, the remote user can be identified with a log in and password and with a certificate if necessary.

15.2 Configuring a TLS connection

The M2Me_Secure software provided by ETIC TELECOM is a Windows TLS client software.

Installed on a PC running Windows XP or Seven, M2Me_Secure makes TLS connections from a remote PC to the RAS-E easy; moreover it includes a connection book in such a way one just need a click to connect to a remote site.

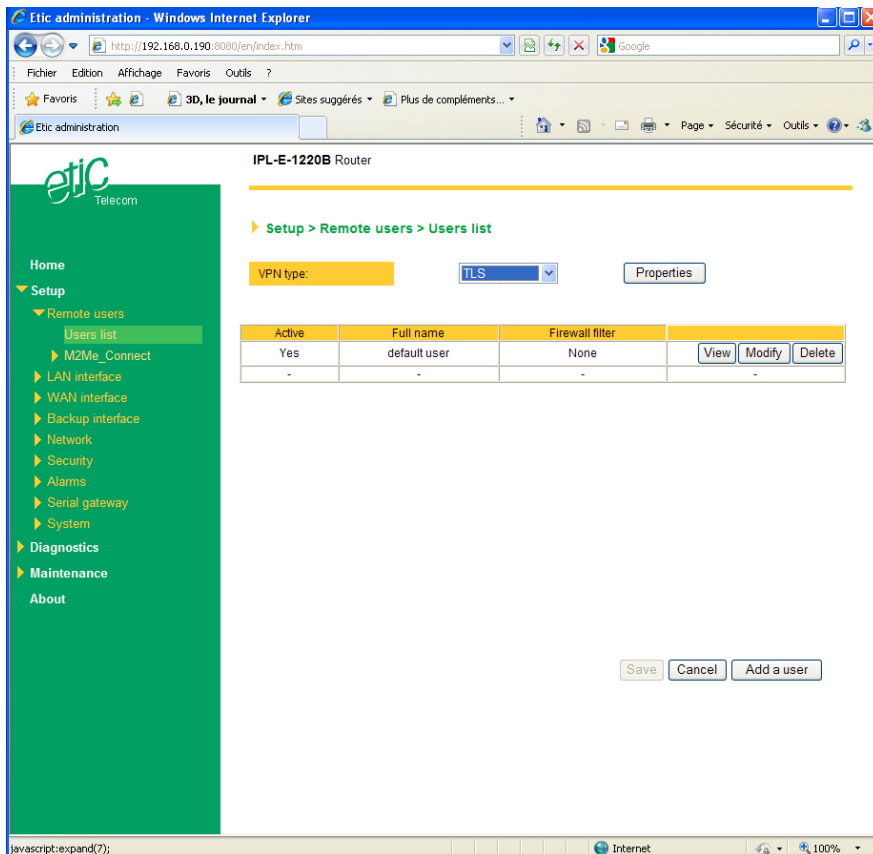
We describe hereafter how to configure the router and the M2Me_Secure software to set a TLS VPN between both.



Step 1 : Router configuration

To configure a remote user TLS connection,

- select the “**Setup**” menu, the “**Remote users**” menu and then the “**User list**” menu.



- Select the VPN type “ TLS”.
- Click the “Properties” button and set the parameters.

”Port number” & “Protocol” :

Select the port Nr and the type of level 3 protocol used to transport the TLS VPN; UDP will be preferred.

Attention :

The selected port number assigned to the remote users connections must be different from the one used for VPN connections between routers if such VPN connections have been configured.

“Remote Users authentication” parameters :

Authentication and encryption can be carried-out with a pre-shared key or a certificate.

If the **“Login/password”** is selected, the remote user is authenticated with a login and a password.

If the **“Login/password and Certificate”** value is selected, the remote PC is authenticated with the certificate and the user with a login and password. In that case, the PC certificate must be stored in the user list.

«Encryption algorithm» & «Message digest algorithm» parameters :

Leave the default values.

Step 2 : Configure the M2Me_Secure software

For detailed information, refer to the M2Me_Secure manual.

- Click « Menu » and then « New site ». The Site configuration window is displayed.
- Select the « General » tab and enter a site name.
- Select the « Connection » tab; select the option “That site can be reached through the Internet.
- In the field « Host name or IP address », select the router IP address or DynDNS name or DNS name.
- Select the « Advanced tab » ; select the level 3 protocol (UDP or TCP), the port number and the encryption algorithm.
These parameters must have the same values must in the PC and in the router.

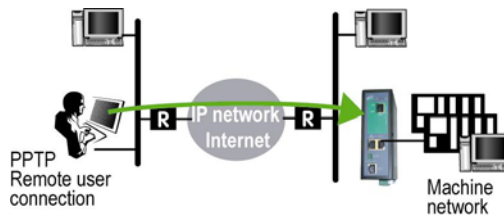
15.3 Configuring a PPTP connection

We describe hereafter how to configure the router and the PC to set a PPTP remote user connection between them.

Step 1 : Router configuration

- select the “**Setup**” menu, the “**Remote users**” menu and then the “**User list**” menu.
- Select the VPN type “PPTP”.

Remark : The “properties” button allows to modify the authentication protocol; leave the default configuration if the PPTP client is a PC running Windows.



Step 2 : Set a PPTP connection on the PC side.

16 M2Me_Connect service

16.1 Overview

The M2Me_Connect service simplifies the connection of a remote PC to a machine through the Internet.

It provides a solution when a direct PPTP or TLS connection described before shows itself impossible.

Let us take the example of a machine made of several devices forming a “machine network” and connected to a company network through an RAS-E router.

Suppose an expert wishes to connect to one or several of these devices to help repairing them or to upgrade a firmware.

The simplest solution should be to set a remote connection between the remote PC and the RAS-E through the company network, the existing Internet access in the company, and the Internet.

Several reasons make that connection difficult or impossible, but the main one is a security reason : It is generally not allowed to set an ingoing connection from a PC connected to the Internet towards a device like an RAS-E connected inside a company network.

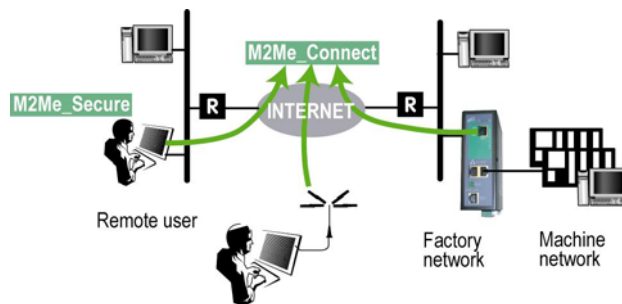
The M2Me_Connect service solves that difficulty :

The PC does not connect directly to the RAS-E; both the PC and the router connect to the “M2Me_Connect” service.

Once both parties have been authenticated by the M2Me_Connect service with their own certificate, a TLS VPN is set from end to end from the PC to the RAS-E router.

The remote user identity is checked by the router to verify he or she belongs to the user list stored in the RAS-E router.

Finally, individual access rights are assigned to the remote user depending on his or her identity.



16.2 Configuring a M2Me_Connect connection

Step 1 : Router configuration

- Select the « **Setup** » menu, the « **Remote users** » menu, the “**M2Me_Connect**” menu, and then the “**Connection**” menu.

« **Activate** » parameter:

Tick the checkbox

“**TCP ports**” and “**UDP ports**” parameters :

Select the ports the router must check to set a connection to the M2Me_Connect service.

Proxy parameters :

If a proxy server is in charge of filtering IP packets transmitted towards the Internet,

select the “Use a Proxy server” option;

choose either “HTTP” or “SOCK S5”;

Enter the Proxy server address, port number, Login and password.

- Test the connection

Click the “Control” menu, and press the “connect now” button.

Go to the “Diagnostic” menu, “Network status” menu and then “M2Me”.

When the connection between the router and the M2Me_Connect service is established, the port number and protocol are displayed.

- Deselect the ports number needlessly selected

If too many ports have been selected, the connection delay may be long; it is why we advise to unselect all the ports except the one which has finally been successful.

Step 2 : Configuring the M2Me_Secure software

- Click « Menu » and then « New site ». The Site configuration window is displayed.
- Select the « General » tab and enter a site name.
- Select the « Connection » tab; select the option “That site can be reached through the Internet and the “M2Me_Connect” option.
- Enter the product key of the router; it can be pasted from the “About” menu of the router.

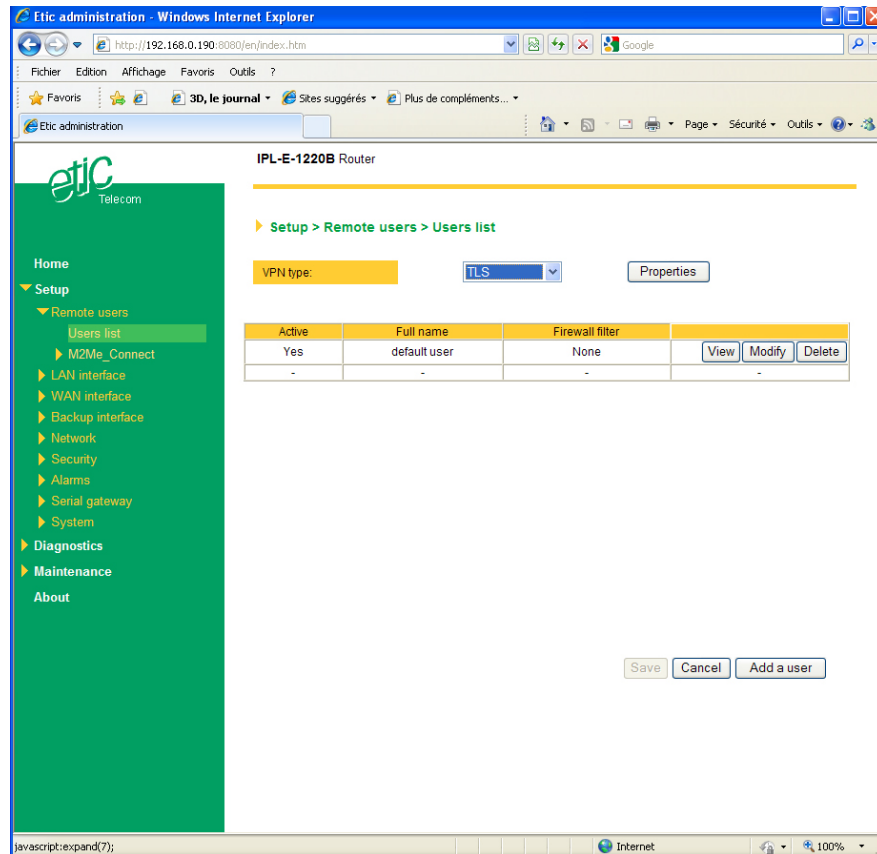
17 Users list

The user list registers 25 authorised remote users forms.

Each user form stores the identity of the user (Login and password), his email address to send alarm emails and the filter assigned to him.

To display the user list,

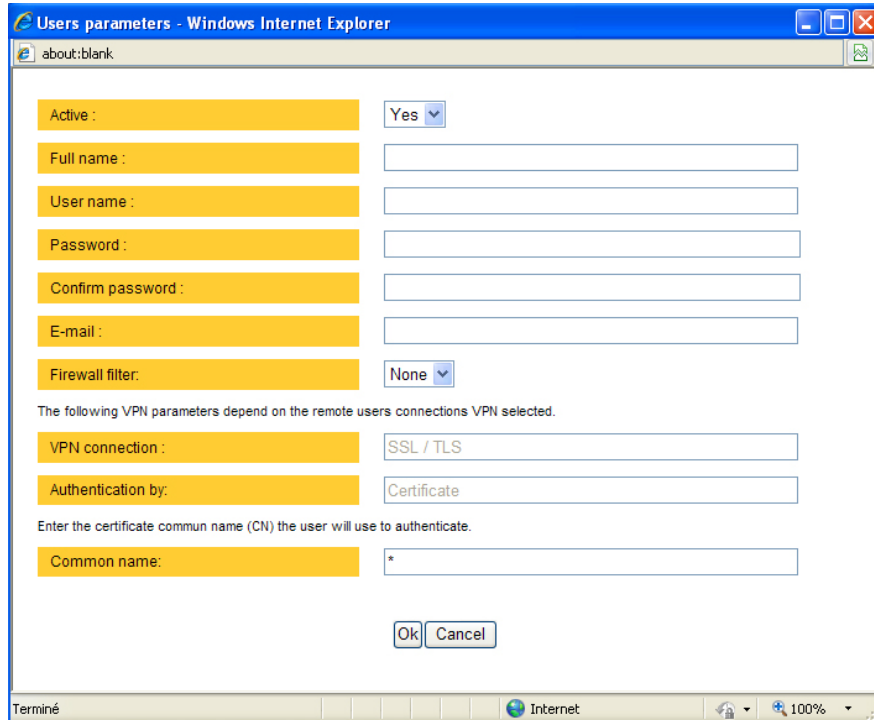
- select the “**Setup**” menu, the “**Remote users**” menu and then the “**User list**” menu.



Attention :

Coming from factory, a default user is registered; his login is **admin** and the password is also **admin**. After the test phase, we advise to modify these login and password.

To add a user form



Users parameters - Windows Internet Explorer

about:blank

Active : Yes

Full name :

User name :

Password :

Confirm password :

E-mail :

Firewall filter: None

The following VPN parameters depend on the remote users connections VPN selected.

VPN connection : SSL / TLS

Authentication by: Certificate

Enter the certificate common name (CN) the user will use to authenticate.

Common name: *

Terminé Internet 100%

- Click the “add a user ” button

“ **Active (value Yes or NO)** ” :

Select “No” if you want to prevent the user to access the network.
Select “yes” to authorize the user to access the network.

Full name :

It is the name displayed in the user list.

Login & password

The login and the password will have to be entered by each user at the beginning of the remote connection.

E-mail :

The RAS-E will send an email to that address in two situations :

Alarm email : the RAS-E sends an alarm email to the defined user If the input 1 is closed or opened (if that option has been set).

Internet connection email : Once connected to the Internet, the RAS-E will send to the demanding user an email containing the dynamic IP @ assigned to the RAS-E by the provider. (See OPERATION chapter).

Firewall filter :

Select a filter in the list.

A filter defines a domain of the local network.

Thus, once assigned to a user, a filter limits his or her access rights.

18 Firewall

18.1 Overview

The firewall filters IP packets between the WAN and the LAN interface of the RAS-E router. It is divided in 3 particular filters :

- **The remote users filters**

The function of the remote users filters is to limit the IP domain an authenticated remote user can reach when he connects to the RAS-E router through the Internet.

The remote users filters filter the destination IP address and port number of the IP packets included inside a PPTP or TLS or L2TP remote user connection.

Thus the IP addresses checked by the remote users filters are LAN IP addresses.

25 remote users filters can be created and assigned individually to each of the users declared in the user list.

The source IP address of the packets is not checked by the remote users filters because the filters apply to the remote users connections according the login and password of the remote user checked when the remote user connection is set.

- **The main filter**

It filters IP packets whether carried inside one of the VPNs or outside a VPN.

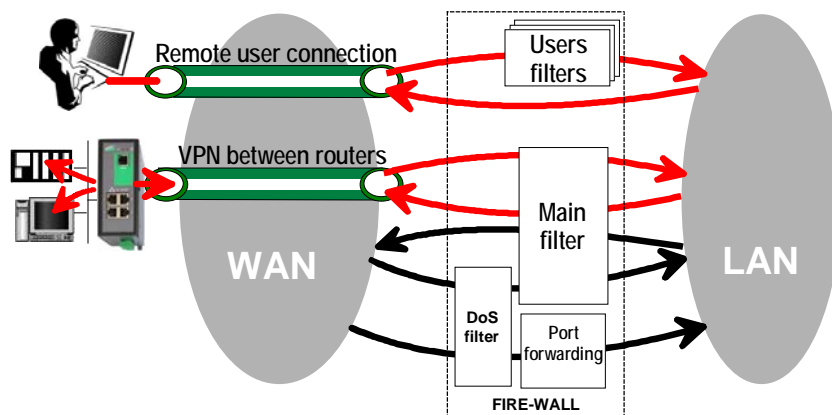
The main filter checks source and destination IP addresses and the source and destination ports.

The main filter does not check the IP packets included in a remote user connection. That packets are checked by the remote users filter.

The main filter does not check the IP packets defined in the "Port forwarding" table. That packets are directly forwarded to the defined device (see [Port forwarding](#)).

- **The deny of service filter** is made to usual attacks coming from the Internet. That filter cannot be configured.

The firewall of the RAS-E firewall can thus be represented by the drawing hereafter :



18.2 Main filter

The main filter applies to all the IP packets except to the ones included in remote users connections.

To recognize a TLS remote user connection, the router detects the port number.

18.2.1 Main filter Overview

- **Main filter structure**

For a better organisation, the main filter is divided in two tables; both having the same structure.

The “VPN” filter : It filter the packets transmitted inside the VPNs.

The “WAN” filter : It filters the packets transmitted outside the VPNs

Each of that two filters is made of

- a filter policy
and
a filter table each line of which is a filter rule

- **Main filter default policy**

The default policy is the decision which will be applied if a packet does not match any of the rules of the filter.

The WAN to LAN and the LAN to WAN traffic are regarded separately because the decision can be opposite for a packet coming from the WAN or coming from the LAN :

WAN to LAN : The default policy can be “Accept” or “drop”.

LAN to WAN : The default policy can also be “Accept” or “drop”.

For instance, if the default policy assigned the WAN to LAN traffic is “drop”, it means that an IP packet which does not match any of the rules of the main filter will be rejected.

- **Main filter table**

The main filter is a table, each line being a rule.

Each rule of the filter is composed a several fields which defines a particular data flow and another field which is called the action field.

The fields which define the data flow are :

Direction (« WAN to LAN » or « LAN to WAN »),
Protocol (TCP, UDP...),
IP@ & port number, source & destination.

The Action field can take two values

Accept : To authorize the data flow to be forwarded to the router interface.
Drop : To drop the packet which matches the rule.

- **How does the main filters works**

When the firewall receives a packet, it checks if it matches the first rule..

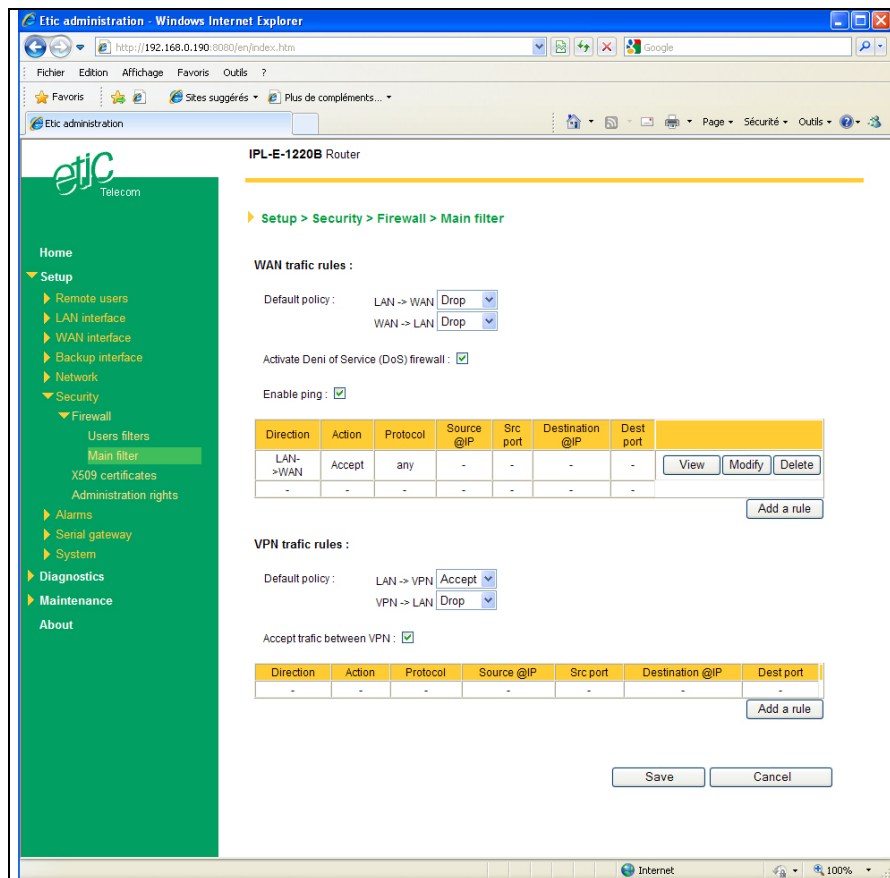
If it does, the decision is applied to the packet according to the "Action" field.

If it does not, the firewall checks if it matches the second rule; and so on.

If the packet does not match any of the rules of the table, the default policy is applied to the packet (drop or reject).

18.2.2 Configuring the main filter

Select the “Security” menu and then “Firewall” and “Main filter”.



The “Main filter” page is divided in two parts :

WAN traffic rules :

The first part, entitled “WAN” traffic rules, is made to define how the IP packets **not carried in a VPN**, have to be filtered.

VPN traffic rules :

The second part, entitled “VPN traffic rules” allows to define how the IP packets **carried inside the VPNs** have to be filtered.

Configure successively the WAN traffic rules using the same method.

Step 1 : Select the default policy

“LAN to WAN” parameter :

That parameter sets what the filter will decide if an IP packet coming from the LAN does not match any of the rules of the filter :

If the value “Accept” is selected, the IP packet will be transmitted to the VPN.

If the value “Drop” is selected, the IP packet will be rejected.

“WAN to LAN” parameter :

That parameter sets what the filter will decide if an IP packet coming from the WAN does not match any of the rules of the filter :

If the value “Accept” is selected, the IP packet will be transmitted to the LAN.

If the value “Drop” is selected, the IP packet will be rejected.

The cautious default policy is to choose the value “Drop”; at the opposite, if the value “Accept” is selected, a frame which does not match any of the rules of the filter is transmitted.

Step 2 : Add a rule to the filter

Click the “add a rule” button.

“Direction” parameter :

Select the direction of the data flow to which the rule applies.

“Action” parameter :

Select the value “Accept” if the IP packet has to be transmitted in the selected direction.

Select the value “Drop” if the IP packet has to be rejected.

“Protocol” parameter :

Select the level 3 protocol concerned.

“Source IP address” & “Source port” parameters :

Enter the value of the source IP address and the source port number.

It is possible to enter a range of source IP addresses and not a single IP address by selecting a netmask value from 1 to 32; It is the number of binary 1 of the netmask; for instance, the value 24 means 255.255.255.0; the value 16 means 255.255.0.0.

"Destination IP address" & "destination port" parameters :

Enter the value of the destination IP address and the destination port number. Select the netmask value.

18.3 Remote users filters

A remote user filter applies to the IP packets received inside a remote user connection.

25 remote user filters can be configured and assigned individually to each of the users declared in the user list.

A remote user filter is a table of destination port numbers and IP addresses belonging to the LAN network.

Once a remote user is connected to the RAS-E router, the router applies the filter assigned to him (see the remote user form).

According to his identity (Login and password, he will thus only access to the IP domain defined by the filter.

Example :

Filter name : Access to the device PLC1 (html and modbus)		
Filter policy : All is forbidden except what we specify		
Rules list		
Action	Device	Service
Allow	PLC1 192.168.0.12	80
Allow	PLC1 192.168.0.12	Modbus 502

A filter must be assigned at least to one user to become enabled.

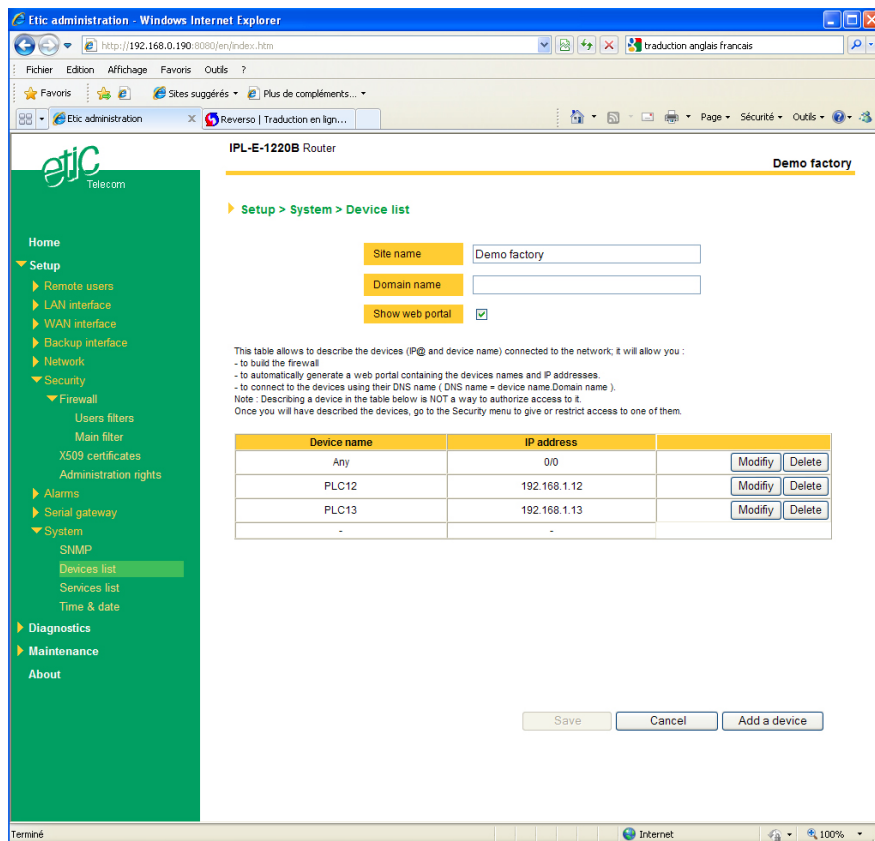
Step 1 : Complete, if necessary, the list of services

Remark : *The main services (html, ftp, modbus) are available from factory; for that reason, most of the time, that step can be skipped.*

- Select the menu "system" and then "service list" The list of TCP ports is displayed.
- Click « add a service ».
- Enter the label of that the new service, assign a protocol (udp, tcp, icmp) and a port number.
- Save. The list is updated.

Step 2 : Enter the list of devices of the LAN network

- Select the «System» menu, then «Devices list».
The list of the devices of the LAN network is displayed.



IPL-E-1220B Router Demo factory

Setup > System > Device list

Site name:

Domain name:

Show web portal: ☒

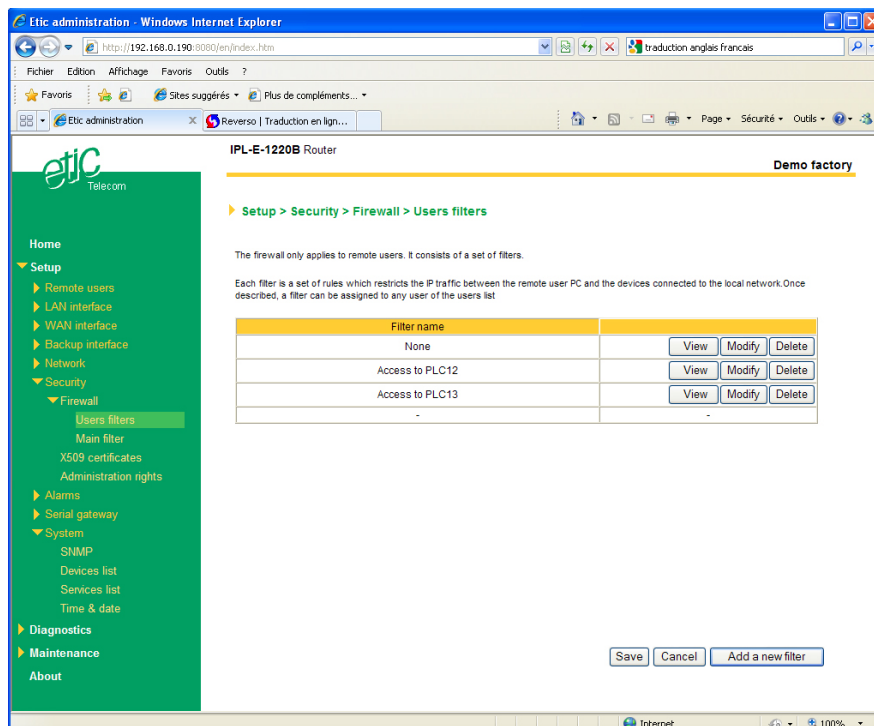
This table allows to describe the devices (IP@ and device name) connected to the network; it will allow you :
 - to build the firewall
 - to automatically generate a web portal containing the devices names and IP addresses.
 - to connect to the devices using their DNS name (DNS name = device name.Domain name).
 Note : Describing a device in the table below is NOT a way to authorize access to it.
 Once you will have described the devices, go to the Security menu to give or restrict access to one of them.

Device name	IP address	
Any	0/0	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
PLC12	192.168.1.12	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
PLC13	192.168.1.13	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
-	-	

- Click « add a device ».
- Assign a label and an IP address to the device and click OK.

Step 3 : Build a remote user filter

- Select the « security» menu, then « firewall» and then «Filter list»
The users filters list is displayed.

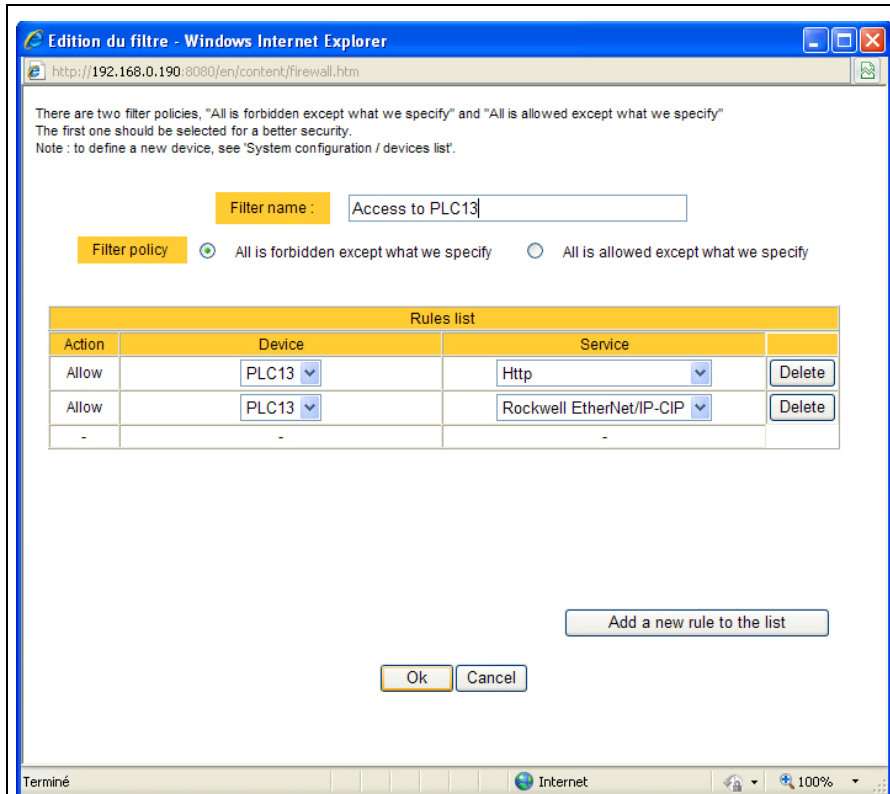


The screenshot shows the 'IPL-E-1220B Router' configuration page in a web browser. The left sidebar contains a navigation menu with categories: Home, Setup, Security, System, Diagnostics, Maintenance, and About. The 'Security' menu is expanded, showing 'Firewall' and 'Users filters' (which is selected). The main content area is titled 'Demo factory' and 'Setup > Security > Firewall > Users filters'. It contains a description: 'The firewall only applies to remote users. It consists of a set of filters. Each filter is a set of rules which restricts the IP traffic between the remote user PC and the devices connected to the local network. Once described, a filter can be assigned to any user of the users list.' Below this is a table with the following data:

Filter name			
None		View	Modify Delete
Access to PLC12		View	Modify Delete
Access to PLC13		View	Modify Delete
-			

At the bottom right of the main content area, there are three buttons: 'Save', 'Cancel', and 'Add a new filter'.

- Click « add a new filter ».



There are two filter policies, "All is forbidden except what we specify" and "All is allowed except what we specify". The first one should be selected for a better security.
Note : to define a new device, see 'System configuration / devices list'.

Filter name :

Filter policy ☒ All is forbidden except what we specify ☐ All is allowed except what we specify

Rules list			
Action	Device	Service	
Allow	PLC13	Http	Delete
Allow	PLC13	Rockwell EtherNet/IP-CIP	Delete
-	-	-	

Terminé

- Assign a name to the new filter.
- Choose the policy ; « All is forbidden except what we specify » is the advised policy.
- Click « add a new rule to the list ».
- Select a device among the ones which have been stored and a service (also called port).
- Add other rules if necessary.
- Click OK when the filter is complete ; the updated filter list is displayed.

Step 4 : Assign a filter to each user

- Select the « Remote user» and then « User list ».
- Select a user to which you want to assign a filter ; and click modify ; the user window is displayed.
- Assign a filter to the user ; click OK and save.

19 Serial to IP gateway

That function is available in RAS-E-1220 or RAS-E-1230

The RAS-E features two serial asynchronous ports RS232 or RS485 (see the [product identification table](#)).

A serial gateway can be assigned to each port .

If the same type of gateway is assigned to both serial ports, the UDP or TCP port numbers must be different.

The gateways listed below are provided :

Modbus client or server (i.e. master or slave)

To connect several serial modbus slaves to several IP modbus clients.
Or to connect a serial modbus master to an IP modbus server.

RAW TCP server or client :

To connect 2 serial devices through an IP network.

Telnet :

To connect a Telnet terminal to the RAS.

RAW UDP :

To exchange serial data between several serial and IP devices, through an IP network, using a table of IP addresses..

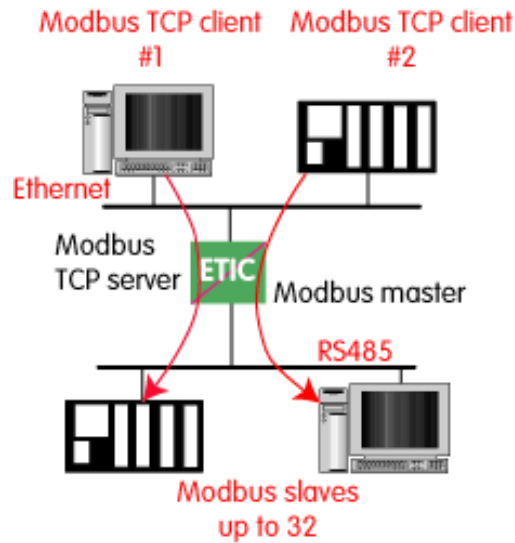
Unitelway slave :

To connect a serial unitelway master to an IP network.

19.1 Modbus menu

19.1.1 Modbus server gateway

This gateway allows to connect asynchronous modbus slaves to the serial interface of the IPRS.



- Select the modbus menu and then modbus server and enable the modbus server gateway and set the parameters as follows :

“Port selection” parameter :

Select the serial port COM 1 or COM2.

If the modbus server gateway is assigned to one serial COM port, it cannot be assigned to the other one.

« ASCII / RTU protocol » parameter:

Select the right option

“Proxi” parameter:

Enable the proxi option if you wish to avoid to frequent requests on the RS232-RS485 interface.

“Cache refreshment period” parameter:

Select the period at which the gateway will send request to the slaves PLC.

“Timeout waiting for the answer” parameter:

Set up the timeout the gateway has to wait for the answer of the modbus slave answer.

“Local retry” parameter :

Set up the number of times the gateway will repeat a request before declaring a failure.

“Inter-character gap” parameter :

Set up the maximum delay the gateway will have to wait between a received character of a modbus answer frame and the following character of the same frame.

“Modbus slave address” parameter:

Choose “specified by the modbus TCP client” , if the address of the slave PLC must be decoded by the gateway from the modbus TCP frame coming from the client.

Otherwise, specify the modbus address of the slave PLC; in that case only one slave can be connected to the RS232 serial interface.

“TCP inactivity Timeout” parameter :

Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

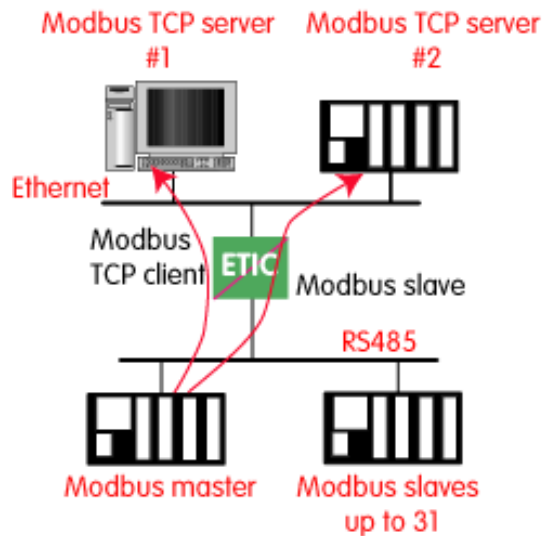
“TCP port number” parameter :

Set the port number the gateway has to use.

If the Raw TCP client gateway is assigned to both serial COM ports, the TCP port numbers must be different on each port.

19.1.2 Modbus client gateway

This gateway allows to connect a serial modbus master to the serial interface of the IPRS.



- Select the modbus menu and then “modbus client” menu; enable the “modbus client” gateway and set up the parameters as follows :

“Port selection” parameter :

Select the serial port COM 1 or COM2.

If the modbus server gateway is assigned to one serial COM port, it cannot be assigned to the other one.

« ASCII / RTU protocol » parameter :

Select the right option

“Inter-character gap” parameter :

Set up the maximum delay the gateway will have to wait between a received character of a modbus answer frame and the following character of the same frame.

“TCP inactivity Timeout” parameter :

Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

“TCP port number” parameter :

Set the TCP port number the gateway has to use.

“IP address” parameter :

The modbus client gateway allows to transmit modbus requests from the serial modbus master device to any modbus slave device, more precisely called “ modbus server”, located on the IP network.

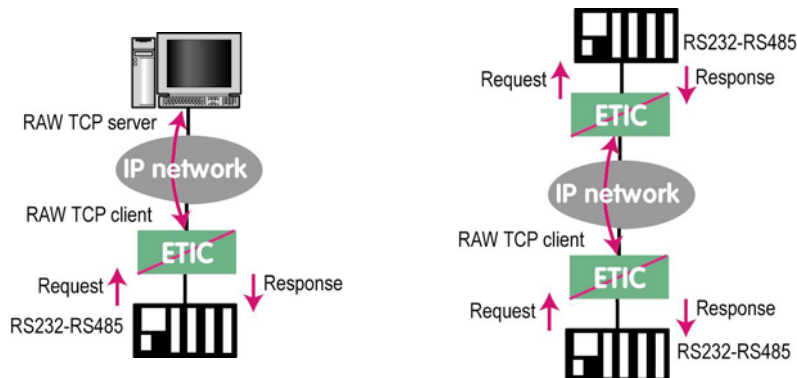
To assign an IP address to each modbus slave device with which the serial master device needs to communicate, click the “add a link” button; Assign an IP address in front of each modbus slave address with which the serial master device will have to communicate.

19.2 RAW TCP gateway

19.2.1 Raw client gateway

The RAW client gateway can be used if a serial “master” device has to send requests to one slave device (also called server) located on the IP network.

The server can be either an ETIC gateway or a PC including a software TCP server.



- Select the “transparent” and then the “raw client COM1” or the “raw client COM2” menu .
- Enable the raw client gateway; and set up the parameters as follows :

“RS232/485 input buffer size” parameter :

Set up the maximum length of an asynchronous string the gateway will store before transmitting it to the IP network.

“Timeout of RS232/485 end of frame” parameter :

Set up the delay the gateway will wait before declaring complete a string received from the asynchronous device.

Once declared complete, the gateway will transmit the string to the IP network.

“TCP inactivity Timeout” parameter :

Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

“TCP port number” parameter :

Set the port number the gateway has to use.

If the Raw TCP client gateway is assigned to both serial COM ports, the TCP port numbers must be different on each port.

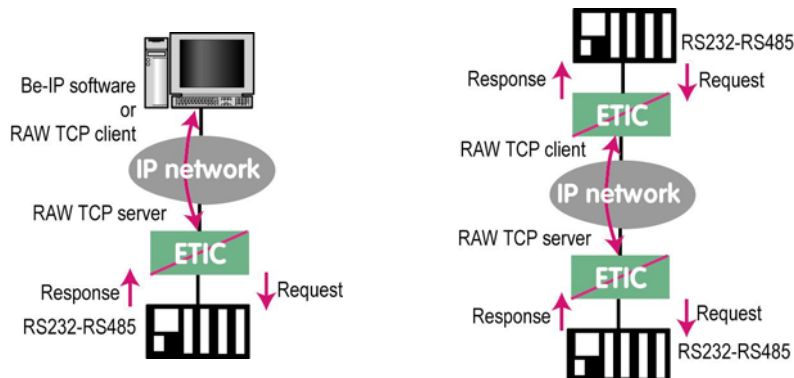
“Raw server IP address” parameter :

The raw client gateway is able to communicate with a raw server gateway.

Assign an IP address to define the destination gateway.

19.2.2 Raw server gateway

That gateway can be used if a serial slave device has to answer requests coming from devices located on the IP network and acting like a master (also called TCP client).



- Select the “transparent” and then the “raw server COM1” or the “raw server COM2” menu.
- Enable the raw server gateway and set up the parameters as follows :

“RS232/485 input buffer size” parameter :

Set up the maximum length of an asynchronous string the gateway will store before transmitting it to the IP network.

“Timeout of RS232/485 end of frame” parameter :

Set up the delay the gateway will wait before declaring complete a string received from the asynchronous device.

Once declared complete, the gateway will transmit the string to the IP network.

“TCP inactivity Timeout” parameter :

Set up the time the gateway will wait before disconnecting the TCP link if no characters are detected.

“TCP port number” parameters :

Set up the port number the gateway has to use.

If the Raw TCP server gateway is assigned to both serial COM ports, the TCP port numbers must be different on each port.

19.3 RAW UDP gateway

19.3.1 Overview

The RAW UDP gateway enables you to connect together a group of serial or IP devices through an IP network.

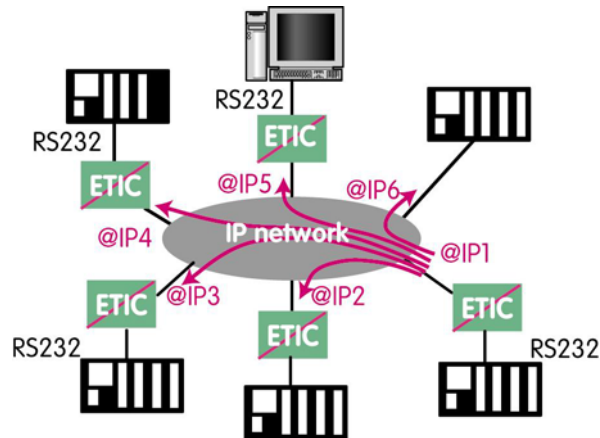
The group can include IP devices if they have the software pieces able to receive or transmit serial data inside UDP.

Serial data transmitted by each device is transmitted to all other serial devices through the IP network.

A table of IP destination gateways is stored in each RAS-E belonging to the group.

The serial data is encapsulated in the UDP protocol.

The UDP frame is sent to each destination IP address stored in the table.



19.3.2 Configuration

- Select the “gateway” menu and then the “Transparent” menu and then click “RAW UDP”.
- Select the “Activate” option.

« Serial input buffer size” parameter (value 1 to 1024) :
Sets the maximum size of an UDP frame.

“End of frame time-out” parameter (value 10 ms to 5 sec) :
Sets the delay the gateway will wait before sending the UDP frame towards the IP network when no characters are received from the serial interface.

«UDP port number» parameter :
Sets the UDP port number.
If the Raw UDP gateway is assigned to both serial COM ports, the UDP port numbers must be different on each port.

“IP addresses of the destination devices » table :
This table stores the IP addresses of the gateways to which the serial data, encapsulated inside UDP, have to be sent.
A different UDP port number can be entered for each destination IP address.

20 USB to IP gateway

That function is available in RAS-E-1201 only.

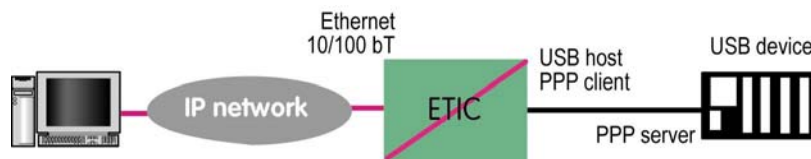
20.1 Principles

The RAS-E-1201 provides a USB to IP gateway.

It is able to forward IP traffic from devices connected to the Ethernet network to a USB device.

On the USB interface, the RAS-E-1201 behaves like a USB host and a PPP client.

The USB device connected to the RAS-E-1201 USB interface must behave like a PPP server.



Destination IP address; main case

When a device, connected to the Ethernet network, needs to transmit data to the USB device, the destination address of the IP frames which need to be transmitted to the USB device must be a specific IP address assigned to the USB gateway of the RAS-E on its LAN nterface (see the configuration below).

Destination IP address; Modbus case

If no specific IP address is assigned to the USB gateway (see below), the RAS-E forwards only modbus TCP traffic to the USB interface. The destination IP address of the IP frames must be the LAN IP address of the RAS-E router.

20.2 Configuration

Select the “Setup” menu and then the “USB” menu.

“Activate” checkbox :

Select the “Activate” checkbox.

“Use a specific IP address” checkbox :

If modbus TCP traffic only has to be forwarded, that checkbox must not be selected.

If other kinds of traffic have to be forwarded to the USB device, that checkbox has to be selected.

“Specific IP address” parameter :

If modbus TCP traffic only has to be forwarded to the USB interface, no IP address has to be entered.

If other kinds of traffic have to be forwarded to the USB device, enter a specific IP address.

That address belongs to the LAN interface network. It is the specific IP address of the USB gateway of the RAS-E.

It will be used as the destination IP address of the IP frames which must be forwarded to the USB device.

“Accept WAN traffic” checkbox:

It is necessary to select that checkbox if the PC is connected to the network connected to the WAN interface.

It is not necessary to select that checkbox if the remote PC is connected to the RAS through a VPN.

21 Advanced functions

21.1 Adding a certificate

Coming from the factory, the RAS-E router includes a certificate delivered by ETIC TELECOOMUNICATIONS acting as a certification authority.

That certificate can be used to set a VPN between two routers.

Two RAS-E routers can set a VPN with one another using certificates only if the certificates have been provided by the same authority.

Additional X509 certificates, provided by ETIC Telecommunications or not, can be downloaded into the router.

To import a new certificate, the file extension can be PKCS#12 with a password or PEM.

Even if more than one certificate have been downloaded into the RAS-E router, one certificate can be used for all the connections.

21.2 Alarms

21.2.1 SNMP

The RAS-E router is able to send snmp traps when alarms occur.

Activation :

If that option is selected, the router will send an SNMP trap if an alarm is detected.

SNMP network management IP address :

Enter the IP address of the management platform

SysName & SysLocation :

That fields allow to identify the source device.

Example :

Sysname : etic

Syslocation : France

Product start-up :

If that option is selected, the router will send an SNMP trap each time it will connect to the Internet

21.2.2 Digital output alarm

If an alarm occurs, the router will open the digital output..

The causes which make the output to open can be either the ADSL disconnection, power input 1 failure, power input 2 failure.

21.2.3 E-mail alarm

When the digital input is closed or opened, an email can be transmitted to one of the users of the users list.

To set that function select the "Alarm" menu and click "email".

Enable the alarm email :

Select this option if you want an email to be sent to a user when the digital input 1 is set ON or OFF.

Alarm launched on event :

If the option OPEN is selected, the alarm will be sent each time the digital input will be opened.

If the option CLOSED is selected, the alarm will be sent each time the digital input will be opened.

If the option BOTH is selected, the alarm will be sent each time the digital input will be opened or closed.

Hold time :

Select the time the input has to stay in its alarm state to be taken into account.

Alarm destination :

Select the user to whom the email must be sent.

Text to send :

Enter the email text.

21.3 Configuring the web portal

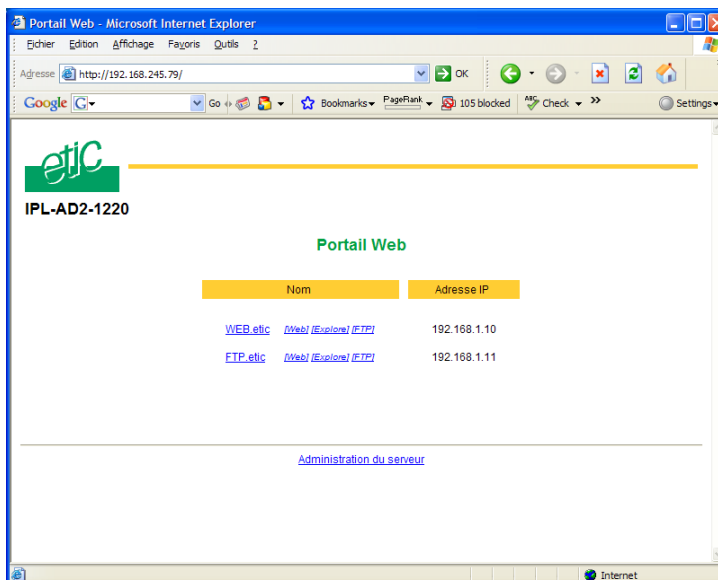
The web portal is an html page; it displays a list of devices connected to the LAN. Each line of the list is made of the device name, its IP address and three links :

The html link : To go directly to the web server of the associated machine.

The « explore » link : To explore the HD of the associated machine, if it is a Windows machine.

The « ftp » link : To explore the files of the associated device.

If the web portal option has been selected (see below), the web portal page is displayed when the remote user launches the navigator and enters the Ip address assigned to the RAS-E router. In that case, the administration server, usually can be displayed at the same address but at the port number 8080 instead of 80 when the web portal page option is not selected.



21.4 Configuring the DNS server

For domain names resolution, the RAS-E can behave like a domain name server or a domain name relay.

DNS server :

A domain name server is a networking device which is able to associate a label (etictelecom.com for instance) with an IP address.

That function allows a client device to send a request to a network equipment referring to a domain name as if it was the actual IP address of the destination device.

The RAS-E router is able to resolve any domain name composed with the name of one of the devices entered in the devices list followed the site name which is entered at the top of the devices list.

DNS relay :

The RAS-E router behaves also like a DNS relay; any DNS request it receives from the LAN, which cannot be resolved because the device is not registered in the devices list, will be transferred to the internet to be resolved.

That function can be carried out only if the RAS-E IP address is pointed out as the main DNS server of the devices of the LAN.

That function is efficient in particular when a device connected to the LAN has to send emails through the Internet.

1 Diagnostic

The html server provides extended diagnostic functions.

Select the Diagnostic menu and then the appropriate sub-menu.

- **Log sub-menu:**

The log displays the last 300 dated events :

ADSL, VPN and users connections and disconnections,
power on,
Serial gateway events.

- **Network status sub-menu and then status sub-menu :**

That screen displays the current status of the LAN interfaces and of the Internet connection :

LAN interfaces :

That part of the page shows the data of the LAN interface :

MAC address,
Ethernet mode (10 /100, half or full),
IP address.

WAN interface :

That part of the page shows the data of the Internet interface :

MAC address,
Ethernet mode (10 /100, half or full),
IP address,
DNS servers addresses
Default gateway

- **VPN sub-menu :**

That menu displays the table of the VPN (remote user connections and remote routers connections) which are established.

- **Serial gateway :**

That page displays the current status of the serial gateways :

Type of the gateway (Modbus, RAW, Telnet ...),
serial port set-up (data rate etc...),
number of characters received or sent,
Number of TCP frames or UDP datagrams received or sent,
Number of TCP connections enabled.

The View link displays a window which shows the hexadecimal received and transmitted traffic over each serial COM port.

- **Ping :**

That screen enables to send a ping frame to an IP address.

- **IO control**

That screen displays the status of the digital input and output and allows to set ON or OFF the alarm digital output.

2 Saving the parameters to a file

Once a product has been configured, the parameters can be stored and restored when necessary.

To save the parameters,

- Select the "System" menu and then "Save restore",
- Click the "Save" button
- Select the location to store the file and give a name to the file.

The file suffix is ".bin".

To restore the parameters,

- Select the "System" menu and then "Save restore",
- Click the "browse" button and select the parameters file,
- Click the "Load" button and confirm to restart the product.

Attention : A parameters file can only be restored towards a product having the same firmware version.

3 Updating the firmware

Step 1 : Before starting, you need,

a PC with a Web browser and an Ethernet cable;
the FTP server software which can be downloaded from the « firmware page » of the ETIC « download area » web server.

Step 2 : Download the release of the firmware from our download area to your PC

Step 3 : Prepare the PC

Check the Ip address of the PC is compatible with the one of the router.

Connect the router to the PC.

Launch the TFTP server (tftp32.exe) software and select the new release (L026xxx/img) by using the "Browser" button.

Click on "Show dir" to check the files of the directory : rfsmini.tgz, rootfs.bin, u-boot.bin and ulmage.

Step 4 : Update the firmware

Launch the web browser

Enter the IP address of the ETIC product ; the home page of the ETIC configuration server is displayed.

Select the "System" menu and then " firmware Update". In the field "IP address of the TFTP server", enter the IP address of your PC.

Note : The IP address of the PC is written in the field "Server Interface" in the TFTP server windows.

Click "Save" and then "Update".

The first file should begin to be downloaded from the PC to the router.

During the operation, the led blinks

When the download is finished, the product automatically reboots.

To be sure the new release has been installed, go to "About" in the administration web page of the IP product.

Step 5 : Restore the default configuration

- Select the "Maintenance" menu and then the "Save / restore" menu.
- Click the "Restore default configuration" button.

1/ Setup menu

Remote users	To assign an ID and PWD to each authorized user and set their rights To set the M2Me service
LAN interface	To enter the IP @ of the router on the LAN interface. To enter the IP @ assigned to the remote users To set up the Ethernet interfaces To set up the DHCP server on the LAN interface
WAN interface	To enter the IP @ of the router over the WAN interface.
Backup interface *	To set up the 3G backup connection
Network	To configures the VPNs To enter static routes and enable the RIP protocol To set up the VRRP redundancy protocol To set up port forwarding To set up advanced Ip addr. translation functions
Security	To set the firewall rules (User filter and main filter) To add a certificate To restrict access to the administration server
Alarm	To set up alarm SNMP traps To set up alarm emails
Serial gateway *	To set up the smodbus gateway (client / server) To set up the RAW TCP / RAW UDP / TELNET gateways To set up the USB gateway (RAS-E-1201 only)
System	To set up SNMP parameters To enter the devices list To update the service list To update time and date

2/ Diagnostic menu

Log To display the events (VPN connections, user connections..)

Network status Interfaces status : @ MAC, @IP, ADSL, VPN
VPN status
Routing tables
M2Me_Connect status

Serial gateways To display the status of each gateway (COM1 and COM2)

Tools To send Pings from the router

Hardware To display the input status
To control the output
To display the DIP switches status

Environment To display the internal T° and the supply voltage

Advanced To store the internal report to a disk for diagnostic purposes

3/ Maintenance menu

Firmware update To update the firmware

Save / restore To save or restore a configuration file
.To restore the factory configuration

Reboot To restart the router

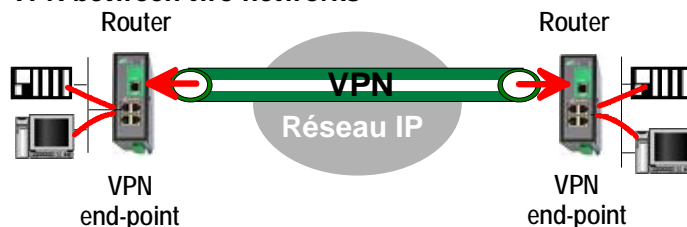
4/ About menu

To display the certificate "product key"
To display the firmware version

1 Overview

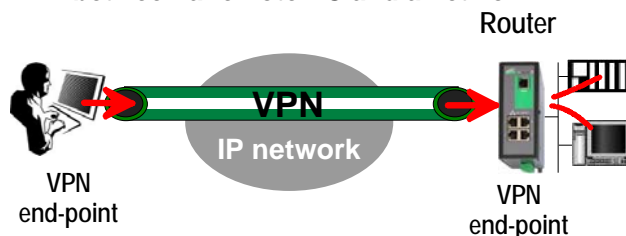
VPN is the acronym for « virtual private network » ; it is a mechanism which allows to connect safely 2 networks together, or 1 remote PC and one network, through a network eventually not intrinsically safe.

VPN between two networks



Once a VPN has been set between the two routers , any device of the first network can communicate with any device of the second one as if the two routers were directly connected with an Ethernet cable.

VPN between a remote PC and a network



2 Functions

A VPN provides the functions described hereafter :

Authentication

The VPN ensures that the party with which the communication is set is actually **the one it claims to be**.

Data integrity

The VPN mechanism ensures that information being transmitted over the public Internet is not altered in any way during transit

Confidentiality

A VPN protects the privacy of information being exchanged between communicating parties.

3 Operation

Authentication phase

The first operation the end-points carry out is authentication.

2 levels of authentication can be performed using a VPN :

Device level authentication

A code is stored in each end-point (i.e. router or PC); it can be a Key or a certificate delivered by a certification authority.

During the initial phase, the two end-point exchange their codes; each party checks that the other party code is valid.

User level authentication

The RAS-E router holds a user list; once a VPN has been set with the remote user PC, the remote user identification code and password is checked.

Encrypted tunnel transmission phase

Once the end-points have exchanged and checked each other identity code, they set the VPN tunnel.

It is an IP packets exchange; the source and destination IP addresses are the end-points. That tunnel encapsulates the encrypted IP data flow transmitted between any of the devices connected to each end-point.

VPN clearing

Periodically, each router (or at least the VPN server router) sends to the other one a control message to check the VPN must remain established.

If no response is received from the other party, the VPN is cleared.

PART 1 : VPN PARAMETERS	
VPN transport protocol : UDP or TCP	
VPN authorized port number among the port numbers hereafter : UDP : 1194 – 5000 – 50001 to 51000 TCP : Idem + 80 & 443	

PART 2 : WAN INTERFACE IP PARAMETERS	
That parameters are not necessary if a DHCP server connected to the factory network assigns automatically its IP address and the other IP parameters to the RAS-E WAN interface.	
IP address assigned to the RAS-E WAN interface over the factory or company network	
IP address of the default gateway over the factory or company network	
Company network netmask	

PART 3 : PROXY SERVER PARAMETERS	
That parameters are necessary only if a Proxy server filters the access from the factory or company network to the Internet	
Proxy Server IP address	
Proxy Server type : HTTP or SOCKS5	
Login for the proxy server	
Password for the proxy server	

Remark :

The network IP address of the devices connected to the LAN interface of the RAS-E must be different

- from the factory network IP address connected to the WAN interface of the RAS-E,
- and from the network IP address of the remote PC.



ETIC TELECOM

13, Chemin du Vieux Chêne

38240 Meylan France

Tel : 33 4 76 04 20 00

Fax : 33 4 76 04 20 01

E-mail : contact@etictelecom.com

Web : www.etictelecom.com